medialaws
Rivista di diritto dei media
1/2018

# Certification Mechanism as a Tool for the Unification of the Data Protection European Law

Giovanni Maria Riccio
*Professor of Comparative Law, Università degli Studi di Salerno*

Federica Pezza
*IP Junior Associate*

## Abstract

The present paper moves from a critical analysis of the new Regulation on Data Protection, which, in the view of the Authors, would not be able to adequately address the complexity of the interests at stake, with the consequence of pre-empting the actual realisation of its harmonisation purposes. Moving from this assumption, the paper looks at the technical measures introduced by the same Regulation and, at this regard, it take into account how the adoption of these rules may foster the construction of a unique legal framework within the EU territory. And in fact technical rules, differently from the legal ones, are not subject to national traditions and to the variables of the interpretative processes. Therefore, the harmonisation purpose of the GDPR, difficult to realise from a strictly legal standpoint, would rather be facilitated from a more technical/formal point of view by means of one of the instruments introduced, namely the certification mechanism regulated by Article 42 GDPR. As we argue, certifications could represent a powerful harmonising tool, acting both as an accountability tool and as a guarantee for cross boarder transfers.

Keywords: GDPR, data protection, certifications, harmonization, accountability

**Giovanni Maria Riccio**
**Federica Pezza**

## Sommario



## 1. GDPR: Expectations vs Reality

Approved on 14 April 2016 by the EU Parliament, the General Data Protection Regulation (GDPR)[1] replaces the previous Data Protection Directive 95/46/EC, with the main purpose of harmonising data privacy across the Europe.

There are two principle reasons behind the Regulation. On one side, it is the reaction to the approach adopted in the previous Directive, often criticised for its excessive flexibility. Differently from Regulations, in fact, Directives are not directly applicable in the Member States, leaving freedom of choice upon their implementation. Arguably, this freedom would not only pre-empt the actual harmonisation, but might even constitute a danger when coming to personal rights as the ones at stake.

At the same time, national regulations and provisions held by Data Protection Authorities have progressively jeopardized the harmonization purposes, making harder the flows of personal data and threatened the commercial exchanges within the internal market.

On the other side, the Regulation represents the effort of taking into account those technological developments that, by enhancing free and multiple flows of data, have the potential to undermine EU citizens' data privacy and, for this reason, require further mechanisms of control. As we will see, the approach followed by the EU authorities in this sense is a risk-based one, imposing a duty on the organisations to preliminary evaluate the possible risks connected to their activities and, if necessary, to put in place the adequate mitigation measures.

One year after its implementation, however, the Regulation does not seem able to fully achieve its aims. Some of the tools and instruments introduced[2], in fact, due to the lack of a clear and specific definition, are still ambiguous and not likely to be interpreted in the same way in different Member States. In other words, despite the efforts of the European Commission, we are still far from achieving a harmonised legal framework and from providing clear and unequivocal rules to the European operators. Also in the light of this remark, the Article 29 Working Party has elaborated a series of guidelines[3], addressing the most controversial areas of the GDPR. The space left to the European and national authorities shows that the Regulation is conceived as a step-by-step legi-

[1] GDPR, *General Data Protection Regulation - Regolamento UE 2016/679* (hereinafter "GDPR").

[2] See for example the notions of Data Portability and Data Protection Officer (DPO).

[3] Namely, *"Guidelines on Data Portability", "Guidelines on Data Protection Officers", "Guidelines on the Lead Supervisory Authority", "Guidelines on Data Protection Impact Assessment"*. For more details see hiip://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

slative process, and that the issue of its final version will be progressively completed.
This paper, although recognising the relevance of similar interventions, moves from the idea that GDPR' ambiguity is the predictable result of its incapability to adequately take into account the expectations of different EU countries. Data protection is, in fact, a controversial area, where social, political and economical considerations all play a role, potentially affecting the unification purpose of the European institutions.
Starting from a comparative approach, the paper will also analyse how national rules have influenced the GDPR and, at the same time, the creation of autonomous rules by the European Commission. In fact, some of the provisions of the GDPR seem to be inspired by a risk based approach, without imposing specific obligations on data controllers and leaving data controllers themselves the assessment of data processing operations and the evaluation of the level of risk and of the security measures to be implemented.
As for the first aspect, the analysis of the German case represents a further confirmation of the possible drawbacks related to the adoption of a liberal approach. The original draft adopted of GDPR, in fact, has already been subject to strong criticism due to the amount of exemptions provided. In particular, it has been noticed that it would not be proportionate. And, because of this, it would result in an unacceptable violation of Article 8(2) of the Charter of Fundamental Rights of the European Union. [4]This is just an example of what can happen when the different actors are given unreasonable freedom in such a delicate area.
The second issue is even more intriguing also because it involves the analysis of the mixture between legal rules and technical (and technological) rules. At this regard, the paper will take into account, in particular, how the adoption of these technical rules may foster the construction of a unique legal framework within the EU territory. The point is that technical rules, differently from legal rules, are not subject to national traditions and to the variables of the interpretative processes.
Starting from these considerations, the present paper argues that the harmonisation purpose of the GDPR, difficult to realise from a strictly legal standpoint, would rather be facilitated from a more technical/formal point of view. Namely, it would take place by means of the instrument introduced, for instance, by Article 42[5] GDPR, a certification mechanism aimed at demonstrating compliance for processing operations by controllers and processors.
This thesis is further validated from the analysis of the current situation. Certification mechanisms, in fact, originally confined to non-legal areas such as sustainability[6], have increasingly been used to ensure compliance also in legal contexts. The latest examples in this sense are certification marks, introduced at the EU level pursuant to the provi-

[4] D. Meyer *Critics: Germany's GDPR implementation riddled with holes, illegalities,* at hiips://iapp.org/news/a/critics-germanys-gdpr-implementation-riddled-with-holes-illegalities/

[5] See Article 42 GDPR and Recital 100 GDPR.

[6] These include Industry Specific Sustainable certifications, internally recognised sustainability standards, ISO 26000 Standards. For more details see https://www.rmagreen.com/sustainable-certifications.

sions of Articles 74a to 74k of the EUTMR[7].
The first path of the present analysis will investigate the main features of certifications, among the already existing international information security standards, which can be applied by the data controllers.
Secondly, the paper will consider the legal effects of applying such certificates, in order to comply with the requirements of the GDPR and avoid or limit the penalties hold by the GDPR. In particular, the paper aims at analysing how certification mechanism may be compliant with regulations concerning risk assessments, data breach notification and privacy by design.

## 2. The role of certifications. Art. 42 GDPR in a nutshell

Chapter 4 of the GDPR, defining the duties of the controller and of the processor, legally formalises for the first time the mechanism of "certification". A first reading of Article 42, in its combination with Article 43 and in the light of Recital 100 of the GDPR, clarifies the main characters of this tool, together with the underlying policy.
First of all, and quite interestingly, certifications are voluntary[8]. The non-legally binding nature of the instrument, however, does not affect its potential for harmonisation. In fact, the same considerations applicable to soft law instruments will come into play in a similar scenario. Namely, voluntary instruments are important as they «often serve as an authoritative way to allow treaty parties to resolve ambiguities in a binding text or fill the gaps»[9].
Secondly, certifications are limited in scope and in time. On one side, they have to be established for «processing operations by controllers and processors». In this sense, the Regulation extends its scope to controllers and processors that are not subject to it within the framework of personal data transfers to third countries or international organizations[10]. On the other, according to Art. 42(7) GDPR «Certifications shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met»[11], in order to ensure updated technological solutions which are effectively able to comply with security and, in general, with data subjects' privacy expectations.
This circumstance, often criticised as imposing an undue burden on the certified bodies, finds its main reason in the need of ensuring constant monitoring. However, the alleged burden is mitigated by the last sentence of Art. 42(1) clarifying that «the specif-

[7] Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amending Council Regulation (EC) No. 207/2009 on the Community trade mark.

[8] On this point, see Article 42(3) GDPR, requiring the certification to be voluntary and available via a process that is transparent.

[9] D.L. Shelton *Soft Law* 2008 GW Law Faculty Publications & Other Works, 2008.

[10] See Article 42(2) and Art. 46(2)(f) GDPR.

[11] See Article 42(7) GDPR.

ic needs of micro, small and medium-sized enterprises shall be taken into account»[12].
This second aspect, by linking the length of the certification to the respect of "the relevant requirements", anticipates the discussion over formalities and procedure. According to Art. 42(5) GDPR, «a certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63».
Two separate remarks are required for understanding this provision. First, a preliminary distinction between issuance of the certification and approval of the relevant criteria and, second, its combination with Art. 43, Art. 58(3) and Art. 63 GDPR.
With regard to the competent certifying bodies, the text of Art. 42(5) leaves two options opened: (a) the competent supervisory authority and (b) the certification body.
Indeed, the first of the two alternative does not require further explanation, as national supervisory authorities (also known as data protection authorities or DPAs) «do not represent a novelty and will continue to exist in Chapter 6 of the GDPR»[13].
In our opinion, however, it is likely that the DPAs will not directly issue certification mechanisms, but will provide the rules to comply with for certification bodies and will validate the certifications already existing or specifically created for ensuring a full protection of personal data.
More issues arise when coming to certification bodies, both for the novelty of the concept and the necessary integration with the text of Articles 43, 58(3) and 63 GDPR.
Schematically, the issuance[14] of a certification from a certification body requires three conditions to be met:
a) certification bodies shall have «an appropriate level of expertise in relation to data protection»[15] (Art. 43(1)GDPR);
b) they «shall provide the competent supervisory authorities with the reasons for granting the requested certification»[16] (Art. 43(5) GDPR).
c) Member States shall ensure that certification bodies are accredited (43(1) GDPR) by the relevant DPA and/or the national accreditation body[17] named in accordance with

[12] The same kind of mitigation applies to Data Portability. According to Article 20(2) GDPR, in fact, «In exercising his or her right to data portability pursuant to paragraph 1 the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible».

[13] Ashurst, *The General Data Protection Regulation(GDPR),* 2017. See also Articles 51-59 GDPR, specifying national supervisory authorities role.

[14] And the renewal. See Article 42(7) GDPR

[15] See Article 43(1) GDPR.

[16] See Article 45(1) GDPR.

[17] More in detail, the main issue in Italy consists in the lack of an authorised national body. In this sense, *GDPR, Il Garante Privacy: "Serve un Provvedimento sulle cerificazioni"*, in *Corriere Comunicazioni*, 2017.

Regulation (EC) No. 765/2008[18].
Notably, like the certification and for the same above-mentioned reasons, also the accreditation is limited in time[19] and it is subject to the requirements set out in Art. 43(2) GDPR[20].
In short, a formal process (the "Job Task Analysis") is undertaken, with the purpose of determining what professional do, under what conditions and with what levels of knowledge and skills. In addition to this, an annual audit is undertaken by the accreditation body and, eventually, this is associated with continuing education.
As a result, the accreditation not only provides a high degree of assurance as to the substance and integrity of the certification program but, because of the professional training associated to it, is also a competitive driver for organizations around the world[21].
In this respect, some legal scholars have pointed out[22] that, for efficiency and scalability reasons, third party certifications by certification bodies should be preferred over certifications by DPAs. In fact, by taking on and sharing the burdens of supervision and oversight with the DPAs, certification bodies would not only reduce DPAs' workload but also protect their functional independence. This conclusion is further confirmed by the evidence that « at this time, it seems like the vast majority of DPAs do not plan to issue certifications themselves»[23].
Turning to "certification criteria", according to Art. 42(5) GDPR (first line, second half), «certifications shall be issued on the basis of criteria approved by the competent supervisory authority or by the European Data Protection Board(EDPB)»[24]. This sentence has to be read together with the previous one. As a result, although certification bodies will be able to issue certifications under certain conditions, they will be anyway subject anyway to the approval of criteria by the DPA or EDPB.
Moreover, Art. 42(5) (second line) specifies that «Where the criteria are approved by the Board, this may result in a common certification, the European Data Seal»[25]. A similar solution, embraced by part of the doctrine[26], looks particularly suitable to our thesis. The adoption of a EU baseline certification, in fact, would allow providing EU wide consistency among different Member States, without sacrificing the need for

[18] According to *CIPL Discussion Paper Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms,* 2017 (hereinafter "CIPL Discussion Paper") **«**to the extent accreditation is performed by national accreditation bodies as opposed to DPAs, such bodies must ensure that their accreditation of GDPR certification bodies are performed by staff with expertise in data protection and other related matters**».**

[19] It lasts for 5 years.

[20] These criteria, however, are yet to be established. Also, according to CIPL Discussion Paper, the elaboration should be open to public comment and industry input before finalisation.

[21] See *Europe IAPP Data Protection Digest*, 13 October 2017.

[22] See CIPL Discussion paper.

[23] S. Meissner, *Privacy Seals: the European Privacy Seals, Europrise*, May 2016.

[24] See Article 42(5) GDPR (first line).

[25] Article 42(5) GDPR.

[26] See CIPL Discussion Paper.

flexibility. In other words, it would be acting as a general framework, whose actual implementation shall take into account the specific organisation and/or context.

## 3. Legal effects

This brief excursus on the certification mechanism codified by Art. 42 GDPR has revealed some of its specific features.

Conceived by the EU legislator as accountability tools, certifications are *voluntary* devices, whose validity is *limited in time and in scope*. Plus, they are *subject to the approval of specific criteria* and have to be issued by *competent bodies*.

In other words, it might be argued, certifications consist in a bundle of limits, clearly contradicting their harmonisation purpose.

Furthermore, certifications may be European or even national, as confirmed by the first paragraph of Art. 42, which encourages the adoption of these tools in particular, but not exclusively, at Union level.

However, in our view, these limitations do not affect certifications' potential as harmonising instrument. Separately, they only contribute in shaping and clarifying certifications' content, by making the monitoring process more effective.

Thus, the claimed unification process would not only be possible but would be a two-fold one, resulting from the combination of two different angles.

On one side, "certifications, seals and marks"[27] constitute a tool for demonstrating compliance and accountability. In this sense, a part from being an element for the authorities to consider when imposing a fine (and the amount of the fine)[28], they would also play a role with respect of specific obligations of the controller or processor[29].

Secondly, in a broader dimension, they «can be used as accountable, safe and efficient cross-border data mechanisms under the GDPR, provided they are coupled with binding and enforceable commitments»[30].

These two perspectives, as we will see below, both constitute the expression of what we regard as the underlying harmonisation aim. In fact, on one side, «by signalling a certain level of data protection (…), certifications could streamline and shorten B2B due diligence processes between certified and non-certified organisations seeking qualified and trusted business partners». By avoiding protracted negotiations about privacy and data security, this would lead to a «greater speed of doing business» within the EU community.

In addition to this, and in the light of our "second angle", their unification role can be extended to cross border transactions. Eventually, in the long term, this mechanism is

[27] In this sense, CIPL Discussion Paper specifies that the EU legislator does not distinguish among the three features.

[28] For more details on the determination of the "if" and the "quantum" see C. McCluskey, *Privacy & Data Protection 2017 GDPR series: fining powers of the supervisory authority,* 2017.

[29] See Articles 24(3), 25(3), 28(5) and 32(3)GDPR.

[30] See on this point CIPL Discussion Paper and Article 46(2)f GDPR.

likely to create and enhance interoperability with other legal systems. This would bring to a significant improvement in geographical coverage and reach.

## 4. Certifications as accountability tool

Discussing certifications role as a tool for demonstrating compliance requires a better understanding of the policy objectives behind the GDPR.
In this respect, it has been noticed that the Regulation «effectively incorporates a risk-based approach to data protection, requiring organisations to assess the "likelihood and severity of risk" of their personal data processing operations to the fundamental rights and freedoms of individuals»[31]. This has been based on the presence of various provisions in Chapter IV of the GDPR referring to "risk" and "risk-assessment", together with Recital 74, clearly stating that measures of controllers should take into account the risk to the rights and freedoms of natural persons. Risk assessment helps organisations to classify processing activities according to their risks to individuals, prioritise compliance and devise appropriate mitigations.
Interestingly, certifications have a role to play in this context and, namely, two complementary functions are involved. First, they act in the physiological phase, *ex ante*. By obtaining the grant of certification, in fact, private sector organisations demonstrate both to the individuals and to the other organisations their compliance with certain standards. In this sense, a part from constituting an element for DPAs' compliance evaluation, Art. 42 is also a factor to potentially increase individuals' trust and confidence in the organisation.
Secondly, certifications can turn into an *ex post* tool, with the purpose of creating and maintaining «verifiable and demonstrable proof of risk assessments in the event of internal or external audits or investigations by the DPA» or/and acting as an instrument to mitigate the risk[32]. If analysed from a liability rules perspective, it can also be noted that these tools may comply with diligence standards that must be respected by data processors and data controllers. However, the GDPR does not provide an automatism, in the sense that the liability of the operators involved in a data processing is subject to a case-by-case analysis, where the adoption of certifications is not considered as a complete proof that exempt data processors and controllers from liability, but as «an element by which to demonstrate compliance with the obligations of the controller».
Therefore, it is not a case if the GDPR expressly refers to the above-mentioned expression in some of its provisions. Namely, Art. 24(3) (responsibility of the controller), Art. 25(3) (data protection by design and by default), Art. 28(5) (Processor) and Art. 32(3) (security of processing) all refer to the certification mechanism, as an element by which demonstrating compliance with specific sets of standards. Similarly, other

[31] CIPL GDPR Interpretation and Implementation Project Risk*, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDP*R, 21 December 2016.

[32] In this sense, other measures were introduced such as pseudonymisation, data minimisation and security.

provisions implicitly refer to this tool, insofar as they mention «measures to mitigate the possible adverse effects». One of these references is in Art. 33, codifying the duty for the organisation to notify personal data breaches to the relevant DPA.

In this regard, it is interesting to specifically address (i) the connection between the certification mechanism and the privacy by design approach under Art. 25(3) GDPR and (ii) its role with regard to the data breach notification.

As known, the notion of "privacy by design (PbD)", codified for the first time in Art. 25, has been used during the last decade of the past century by some scholars[33] and then endorsed by public institutions position papers and national and international acts. Together with Privacy by Default, PbD «operates on the basis of privacy concerns being addressed proactively instead of reactively»*;* in this sense, it has been noticed, this concept would not be about protecting data but designing so that data does not need protection[34].

For this purpose, Art. 35 GDPR integrates Art. 25 text, requiring Data Protection Impact Assessments (DPIA) to be carried out any time a new project processes personal data that are likely to result in a high risk to the rights and freedoms of individuals. Again, in this context, certifications come into play as, «an element to demonstrate compliance »[35],according to the third paragraph of Article 25 [36]. In addition to this, these tools can be included in the list of those «necessary safeguards into the processing» which will act as mitigation measures pursuant to Art. 25(1) GDPR.

With the same purpose of enhancing data security, Art. 33 GDPR codifies the duty for the controller to notify a personal data breach to the relevant DPA. This is not a completely new provision as it was already provided in the EU legislation as well as into national regulations.

According to the above mentioned Art. 33, the notification has to be done «not later than 72 hours after having become aware of it»[37]. The underlying policy is made clear by Recital 88, according to which «a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned».

However, the same art. 33(1) GDPR partially mitigates this principle introducing an exception. This obligation, in fact, has to be carried out «unless the controller is able

---

[33] N. Flannery *GDPR series: a design for life? Design the future of privacy Data Protection Ireland,* in 17(2) *Privacy and Data Protection,* 2017.

[34] *Ibidem.*

[35] See Article 25 GDPR.

[36] However, as made clear in Article 42(4) GDPR **«**A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56**».**

[37] See Recitals 85, 87and 88 GDPR.

to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons». In particular, the Recital requires the demonstration to be «in accordance with the accountability principle»[38].
As a result, the certification mechanism of Art. 42 GDPR, might play a part also in this respect, as an instrument to possibly demonstrate the notification was not necessary. In addition to this, also in this scenario, certifications can constitute a mitigation measure. As such, they would form part of the essential content of the notification, under Art. 33(3)d.[39]
Again, the GDPR does not provide a clear obligation on data processors and data controllers, leaving a space for these subjects to self-judge the measures implemented and to carry on a risk analysis on the breaches occurred.

## 5. Certifications as a guarantee for cross-border transfers

The benefits connected to Art. 42 implementation, going beyond the European legal framework, are likely to positively impact on the future cross-border transactions.
As a general rule, in fact, transfers of personal data to countries outside the EEA may take place if these countries are deemed to ensure an adequate level of data protection[40]. The competent body for assessing the adequacy of protection is the Commission, whose "adequacy findings", in the form of a decision, are binding in their entirety in all Member States. The consequence is that cross-border transfers will be allowed without the need of further protection measures.
The recitals of the GDPR do not clearly explain the reason behind this long standing approach. Recital 101 on one side recognises the necessity of cross-border flows of personal data for the expansion of international trade, on the other states that the level of protection of natural persons ensured in the EU by the GDPR should not be undermined.[41]
The problem of a similar approach is that the list *of "*adequacy findings*"* is currently limited.[42] In addition to this, these assessments are subject to periodic reviews and monitored from the Commission on an ongoing basis. They can be repealed, amended or suspended. Eventually, they might be challenged before the ECJ. This was the case

[38] See Article 33(1) GDPR.

[39] Article 33(2)(d) GDPR describes the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

[40] Loyens & Loeff, *GDPR cross-border data transfers*, 26 April 2017.

[41] E. Ustaran, *GDPR series: international data transfers 2.0,* in 17(5) *Privacy and Data Protection*, 2017.

[42] *Ibidem,* pointing out how «in reality, and given the reduced number of countries that qualify as "adequate", in the majority of cases, controllers or processors wishing to transfer personal data internationally will need to deploy a mechanism that provides appropriate safeguards for the data».

of the US "Safe Harbour" scheme, whose provisions had to be replaced[43] after the well-known *Schrems* case[44].

Art. 46 GDPR provides a set of options for all the situations were an adequacy finding has not intervened. Significantly, this results in more flexibility[45] for both the exporters and the importers of personal data in selecting the data mechanisms that best suits their needs[46].

In particular, in its second period the article states that «the appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by», among the others[47], «an approved certification mechanism pursuant to Art.42»[48] This system, anyway, in order to work, has to be coupled with «binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards». In other words, also in this case, certifications will constitute a necessary (but not sufficient) element for the purpose of the final evaluation upon the validity of cross-border transactions[49].

## 6. Conclusions

The present paper, moving from the incapacity of EU institutions to adequately address data protection harmonisation from a strictly legal standpoint, looks at the certification mechanism introduced by Art. 42 GDPR as a possible tool for the unification process. A similar approach is further validated from the analysis of the current situation, where certifications have been successfully adopted for their guarantee function not only in non-legal but also, and more recently, in legal contexts.[50]

More specifically, this harmonising process would be a twofold one. On the one side, in fact, acting as an accountability tool, certifications can push in the long term toward

[43] EU-US Privacy Shield. See hiip://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605819 for further guidance.

[44] Case C-362/14.

[45] D. Gabel - T. Hickman, *Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation*, in *White & Case*, 22 July 2016.

[46] E. Ustaran, *supra.*

[47] Similar provisions apply to codes of conduct pursuant to Article 40, which, once approved by the competent authority, play the same guarantee function, provided that coupled with binding and enforceable commitments. On this point, it has been noticed that the Binding Corporate Rules (BCR) pursuant to Article 40 would be a de facto form of certification. See Loyens & Loeff, *supra.*

[48] Eventually, in the lack of any of the instruments set out by Article 46(2) GDPR, the same Article 46, in its third period, provides that transfers will be allowed if ad hoc safeguards are contractually agreed, subject to authorisation from the competent supervisory authority". See *Bird & Bird Guide to the General Data Protection Regulation*, May 2017.

[49] Furthermore, in the long term, and provided that the introduction of conflict requirements is avoided, certifications might contribute to the creation of interoperability among different systems of different countries.

[50] Certification marks introduced by Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amending Council Regulation (EC) No. 207/2009 on the Community trade mark.

the adoption of common standards in different organisations within the EU. This would result, *inter alia*, into a greater speed of doing business, avoiding protracted negotiations.

On the other, the text of Art. 46 GDPR is likely to extend certifications' impact beyond the EU Community. The provision, in fact, expressly regards certifications as one of the possible guarantees for cross border transfers, provided that binding and enforceable commitments of the controller are put in place. Eventually, this may lead, in the long term, to the creation of interoperability with other systems of different countries.

In the light of this premise, the potential benefits connected to the certification mechanism are undeniable. In this sense, it has been noticed, by formalising a tool that only existed in practice, the GDPR has the potential to increase the value of such schemes in the eyes of the public, and also in the eyes of organisations.[51]

However, while recognising the positive implications of a similar solution, one has to consider the undeniable difficulties related to its implementation. The evidence in this sense is that «considering the state of play, it is unlikely that certifications will be issued as of May 25, 2018»[52]. Furthermore, for the implementation to be effective, two conditions shall be put in place. If on one side the adoption of an "EU baseline certification" is recommended, on the other the active participation of the private sector organisations will be essential. In fact, while the establishment of an EU wide mechanism would ensure consistency, respecting the differences among the Member States, the participation of private organisations in the elaboration of certification criteria would provide the necessary legitimation to the system.

A positive signal in this direction comes from a recent news release, confirming that «discussions about certifications are continuing(within the Working Party 29) and will be proposed for adoption at the next plenary meeting in February»[53]. These discussions, together with the announced development of new guidelines on data breach notification and DPIA within the Group, might constitute a significant step for the actual implementation of Art. 42 and the realisation of its harmonisation (or rather unification) goal.

[51] *Unlocking the EU General Data Protection Regulation*, *supra.*

[52] S. Meissner, *supra.*

[53] See *Europe IAPP Data Protection Digest*, 13 October 2017.