International Review of Law, Computers & Technology

ISSN: (Print) (Online) Journal homepage: www.informahealthcare.com/journals/cirl20

Certification as guidance for data protection by design

Efstratios Koulierakis

To cite this article: Efstratios Koulierakis (17 Oct 2023): Certification as guidance for data protection by design, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2023.2269498

To link to this article: https://doi.org/10.1080/13600869.2023.2269498

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY
https://doi.org/10.1080/13600869.2023.2269498

Certification as guidance for data protection by design

Efstratios Koulierakis

Law Faculty (Department of Transboundary Legal Studies), University of Groningen, Groningen, The Netherlands

ABSTRACT

Data protection by design is an obligation for data controllers according to article 25(1) of the General Data Protection Regulation (GDPR). The present paper explores the concept of data protection by design and proposes that data protection certificates can offer guidance to data controllers, about compliance with this GDPR obligation. An exploration of officially approved certification schemes shows that the certification requirements may lay down concrete use cases which can guide data controllers about compliance with the obligation of data protection by design. Even though these policies are not a comprehensive guide for data protection by design, they lay down valuable solutions with respect to effective compliance. Moreover, the data protection measures of compliance in certification criteria have been approved by the competent Data Protection Authority and possibly the European Data Protection Board. As the present paper argues, the official approval by the competent authorities creates legitimate expectations under European Union Law. Specifically, data controllers can legitimately expect that abidance by approved safeguards meets the expectations of the authorities that are entrusted with monitoring their compliance. For these reasons, certification though an *ex post* mechanism, can offer valuable *ex ante* guidance.

ARTICLE HISTORY
Received 27 June 2023
Accepted 7 October 2023

KEYWORDS
Data protection by design; certification; legitimate expectations

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a piece of legislation that in many instances contains broad formulations. One such example is the obligation of data protection by design. The idea of data protection by design initially emerged as best practice and nowadays it is clearly articulated as a legal obligation in the current European Union (EU) data protection framework (Al-Sharieh et al. 2018, 175). Specifically, article 25 GDPR obliges data controllers to comply with data protection rules, by design.

The present paper explains, from a legal perspective, whether certification criteria can be a valuable source of guidance in view of the vague obligation of data protection by design under article 25(1) GDPR. It should be mentioned at this point, that there is no

CONTACT Efstratios Koulierakis e.koulierakis@step-rug.nl Law Faculty (Department of Transboundary Legal Studies), University of Groningen, Oude Boteringestraat 18, 9712 GH Groningen, The Netherlands

doubt that certification schemes can be valuable tools for compliance with the principle of accountability in particular, as article 25(3) explicitly mentions. However, officially approved certification criteria may play an important role that goes beyond compliance with accountability obligations. In view of that, this paper only focuses on certification criteria, which are a very specific aspect of the wider certification framework, laid down in articles 42–43 GDPR.[1]

Article 25(1) lays down some abstract requirements for data controllers.[2] The open-textured expressions that are part of article 25(1) are a means for regulators to deal with the dynamic environment of technological change. The role of open-textured terms in the domain of technology regulation has been addressed by Ronald Leenes (Leenes 2019). In connection to these broader considerations, the present contribution explores the added value of officially approved certificates, in relation to the interpretation of these abstract formulations. The need for authoritative guidance in view of data protection by design has already been drawn out in the legal doctrine (Bygrave 2017, 117). It should be mentioned that according to the initial proposal for the GDPR, the Commission would have been able to adopt delegated acts, 'specifying any further criteria and requirements for appropriate measures and mechanisms, … for data protection by design requirements applicable across sectors, products and services' (EU Commission 2012, art. 23(3)). This provision did not make it to the final text of the GDPR, but it shows that the drafters of the first proposal were aware of the need for authoritative guidance, in view of the abstract requirements of data protection by design. It is yet to be discussed in the legal doctrine, whether certification criteria can serve such a function, in relation to the obligation of article 25(1) GDPR. The argument that this paper introduces is the following: data protection safeguards, which have been officially approved as certification criteria may function as an authoritative source of guidance as to how one can incorporate data protection principles in the design of software, which can reach as far as providing quantified benchmarks for data controllers. In that regard, the official approval of data protection safeguards in certification criteria by the competent Data Protection Authority (DPA), creates legitimate expectations on behalf of data controllers.

After this introduction, the paper analyses article 25(1) GDPR, from a legal-doctrinal perspective and further shows that unclarity about data protection by design derives from the lack of references to specific measures and the need for a balancing exercise, for the identification of the necessary safeguards of compliance. After this analysis, the paper briefly presents the certification regime of the GDPR and explains that certification criteria may include references to specific safeguards of compliance with data protection by design. Subsequently, the text elaborates on the authoritative character of the approved safeguards vis-à-vis of the principle of legitimate expectations under EU law, in order to showcase the legal value of guidance through certification criteria. In the last section, the conclusions of the present work are presented.

Data protection by design

In a digital environment, the architecture of applications is of pivotal importance for the conduct of persons. This is because the architecture of digital applications channels human conduct towards specific actions (Hildebrandt 2008, 174). As the architecture of digital applications is of particular importance in the domain of data protection, article

25(1) GDPR seeks to shape technology in a way that it incorporates data protection values (Bygrave 2020, 573). Article 25(1) GDPR requires that data controllers should actively take both technical and organisational measures to embed data protection principles in digital applications (Jasmontaite et al. 2018, 173). This requirement, however, immediately begs the question of what kind of measures data controllers should implement and what kind of technological solutions they should deploy in that regard. Article 25(1) GDPR gives no direct answers to these questions and it turns out that the process of identifying the appropriate technical and organisational measures, is a complex interpretative exercise.

Lack of references to specific measures

The first challenge that one might face while interpreting article 25(1) GDPR is the lack of guidance by the EU legislator as to which technological solutions one should implement and how (Koulierakis 2022, 36). It should also be pointed out that the GDPR is a relatively new piece of legislation and it still lacks an extensive corpus of case law by the European Court of Justice (ECJ), which can guide its interpreters. It is notable however that, as the report of the Future of Privacy Forum indicates, there are already a significant number of cases where EU DPAs have already addressed questions of the application of article 25 (Michelakaki and Vale 2023). Despite significant improvements in case law, article 25 GDPR remains a (relatively) new provision, and its addressees still lack detailed measures of compliance.

In that regard, article 25(1) mentions the requirement of adopting technical and organisational measures, but it does not go into detail about what technical and organisational measures one should implement and how. Furthermore, it makes no specific reference to technological solutions, specific standards or any other procedures or data protection policies. The only exception is the method of 'pseudonymisation', which is mentioned explicitly. However, it is only an indicative example. Thus, while it is not always necessary for data controllers to implement pseudonymisation techniques, equally the implementation of pseudonymisation does not necessarily secure compliance with article 25(1).

Apart from pseudonymisation, it is up to data controllers to further investigate other available measures and to choose how they will meet the prerequisites of article 25(1). It becomes apparent at this point that it is up to controllers to identify which technical and organisational safeguards are appropriate in their case as well as to identify how the necessary safeguards should be implemented, within the context of their own processing activities. In other words, article 25(1) describes a desirable end-result, which is the incorporation of safeguards that effectively protect the rights of the data subjects (Jasmontaite et al. 2018, 173). However, the provision offers little guidance about how data controllers can achieve this desired end-result.

It remains up to data controllers to interpret article 25(1) GDPR, to identify the appropriate technical and organisational measures, and to effectively incorporate data protection principles into digital applications. Of course, this choice by data controllers goes hand-in-hand with the scrutiny of the DPAs. It is up to data controllers to choose how they will comply with article 25(1) and it is up to DPAs or the judiciary to decide whether data controllers have achieved the desirable outcome.

While it is up to data controllers to identify the best means of compliance with data protection by design, they lack authoritative guidance and hence article 25(1) GDPR is

a source of uncertainty. More precisely, the absence of references to specific standards or data protection technologies creates uncertainty for stakeholders in the tech-industry, about which specific technical and administrative measures would suffice for compliance with article 25(1). This vague formulation comes with a large benefit, because the absence of references to specific technical solutions or standards enables legislators to regulate technological challenges in the future, which had not existed at the time of adoption of the legislation (Leenes 2019, 14). Moreover, it enables data controllers to create new technological solutions. However, this flexibility comes at the cost of clarity.

The need for balancing potential risks against appropriate measures

It is clear at this point that the incorporation of safeguards in the processing of personal data is the desired outcome of article 25(1) GDPR. Even though the article does not prescribe the means of achieving the desired outcome, it offers some guidance as to what qualifies as effective data protection by design. In that regard, the provision mentions that when implementing technical and organisational measures, data controllers should take into account: 'the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'. Thus, it enumerates the necessary elements according to which there should be an evaluation of what qualifies as effective compliance by design (EDPB 2020, 7–8). As further analysis shows, the evaluation of effectiveness is a product of a balancing exercise, which has to take place with regard to the particularities of the context of personal data processing.

Specifically, article 25(1) adopts a risk-based approach, in the sense that the identification of the appropriate means of compliance with data protection rules depends upon the risks to the data subjects (Jasmontaite et al. 2018, 177; Bygrave 2020, 576; EDPB 2020, 9). This risk-based approach requires that the higher the risk to the data subjects, the stricter the measures that data controllers should implement. Hence, the identification of the appropriate measures of compliance with article 25(1) is the product of a balancing exercise, in which technical and organisational measures are adopted in order to counterbalance the risks to the data subjects. When it comes to balancing rights and interests, this is always a challenge for lawyers, and there can be an element of uncertainty as to which outcome strikes a fair balance between the competing interests. The lack of common understanding in relation to what kind of potential harms should be taken into account as risks (Kuner et al. 2015, 97), adds to the difficulty of the interpretative exercise.

Specific measures in certification criteria

The present section explores the value of certification requirements with regard to the challenges identified in relation to data protection by design, particularly the lack of references to specific measures and the uncertainty pertaining to the balancing exercise. In that regard, there is ground for further discussion as to how the reflections on article 25(1), that form part of certification criteria, can be useful as a source of guidance for data controllers. As further analysis suggests, certification requirements, that have been approved in accordance with article 42 GDPR, on some occasions lay down very precise specifications of measures of compliance by design.

Data protection certification in brief

According to article 42 GDPR, data protection certification can be understood as an attestation by a third party, according to which the processing operations by a data controller meet the requirements of the GDPR (EDPB 2019, 8).[3] The outcome of certification is a statement of conformity by a third party, which can be referred to as a data protection certificate (EDPB 2019, 8). The attestation of conformity by the certifying party should take place in compliance with pre-determined criteria.

The GPDR makes no reference as to who should develop the certification criteria. They might be drafted by DPAs, but this is not necessary. Entities other than DPAs may draft their own certification schemes and subsequently submit them for approval to the competent DPA. In the EDPB's terms, these entities are referred to as the 'scheme owners' (EDPB 2023). Even private companies that are not in charge of issuing data protection certificates themselves can be scheme owners (EDPB 2023, 3). In any case, a GDPR certification is officially approved by the competent DPA, no matter who drafts the criteria (GDPR, art 42(5)). Moreover, article 42 GDPR lays down a procedure for the approval of the certification criteria by the EDPB, at the EU level.

The scope of a certification scheme and thus the scope of the relevant criteria can be either general or sector-specific. In the words of the European Data Protection Board (EDPB), 'certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR … ' (2022a, 4).

According to article 42(4) GDPR, a data protection certificate can be issued by the competent data protection authority or by a certification body. Certification bodies are private bodies. These bodies can undertake certification as a commercial activity (Rodrigues et al. 2016, 260). Unlike the data protection authorities, there can be concerns as to whether private bodies have the knowledge, abilities, organisational structure and impartiality guarantees to deal with the monitoring of data protection compliance. For that reason, when it comes to certification bodies, there is the process of accreditation, a process for 'certifying the certifiers' (Kamara and De Hert 2018, 18). This process is laid down in article 43 GDPR which further describes how a certification body can get accredited as such (Rodrigues et al. 2016, 254).

Hence, the GDPR creates a framework, that enables data controllers to prove compliance with the GDPR in general, and article 25 GDPR in particular. The formal mechanism of compliance demonstration is a tool that satisfies the accountability requirements of article 25 GDPR (GDPR, art 25(3)), and it further awards certified controllers by reducing fines, in the case of a GDPR violation (GDPR, art 83(2)(j)). However, despite the added value of data protection certificates for certified parties themselves, the regime of article 42 GDPR might also offer guidance, by specifying the abstract requirements of article 25(1) GDPR.

GDPR-CARPA

GDPR-Certified Assurance Report-Based Processing Activities Certification Criteria (GDPR-CARPA) is the first officially approved scheme in accordance with article 42 GDPR. This particular scheme has been drafted and approved by the DPA of Luxemburg. The same

authority accredits certification bodies, which subsequently issue the data protection certificates (EDPB 2022d).

As a general certification scheme, it is applicable across all sectors of personal data processing. The drafters of GDPR-CARPA certification criteria have formalised GDPR compliance in specified actions that a controller should undertake. In fact, abiding by the certification criteria means undertaking these specified actions. In other words, there is a change in the perspective in comparison to the text of the GDPR: instead of raw legal provisions, the scheme contains a step-by-step approach that, if followed by data controllers, secures compliance with the Regulation.

Most requirements in GDPR-CARPA are generic and up to a large extent they reiterate the provisions in terms of actions that should be undertaken. For example, the scheme requires that the entities should 'design policies and procedures that shall cover … the obligation of data protection by design' (CNPD 2022a, sec. I–2). Thus, when a data controller is certified as compliant with this scheme, there has been an overall overview of their processing operations as compliant with the GDPR in general, and article 25(1) in particular. From this perspective, certification of this type is a useful accountability tool, but not a valuable means of guidance.

However, there are certain instances where the scheme specifies the abstract requirements of the GDPR. Notably, that is the case with training and awareness programmes for personnel. According to section I-16, data controllers should organise a 'data protection training and awareness programme … which corresponds to the competency requirements defined for each role / position' (CNPD 2022a). The criteria further require that 'the entity ensures that each employee and external staff follows these sessions at least once a year and documents their participation accordingly'. The same section of the scheme further specifies that the entity that aspires to be certified needs to assess 'the competencies and experience of the [personnel] to ensure that they meet the requirements for their specific role. This assessment shall be carried out on an annual basis and shall be documented'.

GDPR-CARPA does not explicitly classify these actions as measures of compliance with article 25(1) GDPR, but as the EDPB clarifies, personnel training programmes constitute an organisational safeguard of data protection by design (2020, 6). In that regard, GDPR-CARPA offers some clarity as to what kind of organisational measures article 25(1) requires. For example, it becomes apparent that internal training programmes are important in view of the general principles in the GDPR, and that it is sufficient that employees are assessed annually in relation to the knowledge that they gained. This assertion is a valuable clarification, even though the GDPR-CARPA scheme does not go as far as to clarify the content of training programmes.

These criteria are a necessary requirement for certification but they also offer some clear-cut guidance in relation to article 25(1). Even though GDPR-CARPA specifies that training programmes and evaluation of personnel are useful organisational measures, the scheme is by no means a comprehensive guide about compliance with the obligation of data protection by design. For example, it does not specify any concrete policies about which employees should get access to specific directories with personal data. However, a data controller who aspires to get certified with GDPR-CARPA has some very clear-cut guidance, about the importance of training and evaluation activities, as an organisational measure of compliance by design. In that sense, the scheme lays down specified

actions of compliance by design, which (as discussed already) are not explicitly mentioned in article 25(1).

These specifications in GDPR-CARPA are also relevant to data controllers who (for whatever reason) do not opt for a certificate. In view of the standardised practice laid down in the scheme, all data controllers have some clear-cut indications about the way they should design their training and evaluation procedures. Specifically, the criteria in GDPR-CARPA clarify that annual evaluation of personnel is a best practice in view of compliance with article 25(1) GDPR. This best practice does not imply that all data controllers have the duty to adopt training programmes for their personnel. It does not mean either that compliance with this particular practice exhausts the organisational duties under article 25(1) GDPR. However, the scheme contains a use case that requires that data controllers should make an assessment once every year. In that sense, the criteria lay down a particular action of compliance with article 25(1) GDPR that is useful for any data controller, not necessarily the ones who aspire to get certified.

Age appropriate design

As far as the assessment of the risks to the data subjects, a sector-specific certification scheme can identify risks to the data subjects that arise in a particular societal context and further guide data controllers about the necessary measures of compliance. A very illustrative example in that regard is the protection of minors in the Certification Scheme on Age Appropriate Design, which has been approved by the UK Information Commissioner's Office (ICO) (Age Check 2021). Even though the UK is no longer a EU Member State, it applies the same data protection standards, the rationale behind certification is relevant, and the conclusions of the examination of the scheme can be easily transposed to data protection certification within the EU. The owner of this particular scheme is Age Check, a private entity which also functions as the certifier for the purposes of the scheme (UK ICO n.d.).

This scheme of Age Check certifies data processing operations of any information society services likely to be accessed by children (2021, 7). Hence, this particular scheme (unlike GDPR-CARPA) is sector-specific, as it focuses on technologies that have a very specific characteristic, which is that the services are appealing to children. Due to its specificity, this particular scheme offers very granular policies in relation to the appropriate design of these applications. That is because this sector-specific certificate takes into account some social parameters of personal data processing (which is the likelihood of an application to be used by minors) and elaborates on technological solutions that are better suited to address the legal challenges deriving from that context.

For instance, data controllers have the duty to assess whether the data subjects are adults or not (Garante per la Protezione dei Dati Personali 2023). In view of that, the Certification Scheme on Age Appropriate Design mentions that data controllers may '[use] artificial intelligence to analyse the way in which the user interacts with their service', in order to identify the age of the data subject (Age Check 2021, 28). To that purpose, the text refers to specific standards which quantify, in very precise terms, the reliability of such artificial intelligence solutions (Age Check 2021, 28; 2020, 20). For example, in a sample of 299 persons, the reliability of the artificial application on age check should be 99% (Age Check 2020, 20). This example shows that certification requirements can

quantify measures that are designed to address the threats to the data subjects. The quantified result seems to take into account the legitimate interest of data controllers to undertake the specified activities, as well as the need for protection of minors who are likely to access the application. This balancing act implies that the drafters of the scheme have reflected upon the question of how the existing technical solutions address the need for an age check in certain applications.

As the example of the certificate for age appropriate design indicates, certification criteria can be very specific as to what are the design requirements of digital applications. In the example discussed above, the reliability of the age check algorithm is a certification requirement but its value goes beyond the certification mechanism. In the first place, it clarifies that there is a duty to conduct an age check, in relation to services that are likely to be accessed by minors. The certification requirements further clarify that in view of this obligation, one can adopt artificial intelligence solutions, in order to automate this check. Most importantly, the certification scheme goes as far as clarifying technical requirements of such a solution in terms of quantified prerequisites.

As argued thus far, the effectiveness of a measure of compliance is evaluated on a basis of a balancing exercise and in that regard, it is very hard (if not impossible) for any interpreter of article 25 GDPR to propose a value that satisfies this effectiveness test. However, as the Age Check example shows, certification criteria can reach as far as proposing quantified benchmarks in the form of certification requirements pertaining to the design of digital applications. Hence, certification criteria can give some clear examples to data controllers, as to which measurable outcomes they should achieve, when they determine the safeguards of personal data processing.

Interim conclusion

Thus far, the analysis of existing schemes shows that certification requirements may specify the abstract requirements, that one might need to follow for complying with data protection by design. Even though certification schemes are not originally designed to offer clarifications on the necessary technical and organisational measures, guidance can be a valuable byproduct of GDPR's certification regime. The idea that data protection certification can offer guidance to data controllers, who do not (necessarily) aspire to get certified, does not disregard the added value of data protection certification, as an attestation of compliance. Still, data protection certification is a valuable tool for proving compliance, in accordance with the principle of accountability (GDPR, art 5(2), in conjunction with article 25(3)). However, setting aside the question of *how one proves compliance*, certification criteria can offer valuable clarifications on the question, *how one can comply with article 25(1) GDPR*.

As the example of Age Check shows, sector-specific schemes can take into account the particularities in a specific domain of activities and they might reach as far as providing quantified benchmarks about technical measures of compliance with article 25(1) GDPR. Despite that, as the example of annual evaluation in GDPR-CARPA shows, even general certification requirements can lay down concrete measures of compliance by design.

This conclusion should not be understood as implying that abidance by officially approved certification criteria secures compliance with article 25(1) GDPR. The drafters

of certification requirements cannot predict all possible instances of processing and thus the certification criteria cannot cover all possible instances of violations of article 25(1) GDPR. This means that even if the certification criteria specify data protection policies in a very detailed manner, there might still be instances which are not sufficiently captured by the data protection safeguards laid down in certification schemes. This holds true, irrespective of the degree of specification of the certification requirements.

Despite this conclusion, the examples presented in this section illustrate the value of certification criteria as guidance for compliance by design. Even if the totality of data protection requirements cannot be captured in the form of clear-cut certification requirements, one can identify concrete use cases that give very specific examples of technical and organisational measures of compliance by design. Hence, even though GDPR certification is (currently) in an early stage of development, it is already a valuable, publicly available source of guidance in relation to the obligation of data protection by design.[4]

The authority of certification criteria

It remains to be seen what is the value of the guidance offered in certification criteria from a legal perspective. In that regard, the drafting process of certification schemes is very important. As already presented, certification criteria are always subject to the approval of the competent DPA. As further analysis suggests, the official approval turns the data protection policies in the criteria into authoritative texts. This section further investigates the legal value of the authoritative approval, from the perspective of EU law and it juxtaposes the schemes developed in accordance with article 42 GDPR vis-à-vis other standards.

Reassurance deriving from the authoritative approval

The approval of the certification criteria by a DPA is a reassurance of quality, because of the qualifications of DPA members that are prescribed by the law (GDPR, art 53(2)). For example, a data controller who seeks to comply with article 25(1) GDPR might decide to adopt the measure of annual assessment of the personnel required by GDPR-CARPA, not (necessarily) because they aspire to get certified, but because they trust a practice that has been approved by a DPA.

However, the authority of certification criteria goes beyond that, because specific safeguards meet the expectations of the very same authorities that are entrusted with monitoring their compliance. In other words, data protection authorities should not change their minds arbitrarily, in view of the value of specific technical and organisational measures, as long as they have already approved such measures in the form of policies expressed within a data protection certification scheme.

Let us focus on the example of the annual assessment of personnel. This organisational measure has been approved as a best practice, applicable across different sectors of personal data processing (CNPD 2022a, sec. I–16). Let us imagine that a diligent controller adopts the organisational measure of training programmes accompanied by an annual assessment of the personnel. One may expect that the very same DPA who approved this policy will not suddenly change their views and require that the assessment of personnel should take place bi-weekly.

It might be the case that the controller in the previous example chooses to assess their personnel on their data protection knowledge biannually. In the very particular instance of that controller, it might be the case that a biannual evaluation is a sufficient safeguard in accordance with article 25(1) or that there is no need for training programmes at all. However, if the data controller opts for the biannual assessment (or no training programmes at all), then that choice is of their own and it would lack the authoritative approval by the competent DPA. In that case, the data controller is not reassured that their understanding of data protection by design is also the one of the competent authority.

By the same token, let us imagine that a DPA approves a certificate that contains an age check requirement that has 99% reliability in a sample of 299 data subjects, similarly to the Age Check scheme in the UK. On the basis of such a standard, a data controller may expect that a tool with reliability 99.9% on a sample of 299 persons, also meets the expectations of the competent DPA. This holds true, regardless of whether a data controller is a certified party under the scheme or not.

The principle of legitimate expectations in EU law

The authoritative approval of clear-cut technical and organisational measures, in the form of certification criteria, is very important in view of the principle of legitimate expectations, which forms part of the EU legal order (*Milchkontor ao* 1983, para 30). The principle can be understood as requiring that:

> community legislature and the other Community organs (or the national authorities operating under provisions of Community law) … exercise their powers … in such a way that situations and relationships lawfully created under Community law are not affected in a manner which could not have been foreseen by a diligent person. (AG Cosmas in *Duff ao* 1995, para 25)

Especially in relation to the national authorities, the ECJ has recognised that the principle of legitimate expectations is applicable to them, as long as they implement EU law (*Vereniging Nationaal Overlegorgaan Sociale Werkvoorziening ao* 2008, paras 52–53). Therefore, the principle is relevant when it comes to DPAs implementing the GDPR.

It should be pointed out that legitimate expectations might arise from documents which are issued by public authorities, even though those texts are not necessarily laws in the typical sense. Specifically, it is often the case that public authorities often self-impose rules about how they will exercise their powers, in accordance with general legal provisions (Senden 2004, 406). Such self-imposed rules by public authorities might have a binding effect on them, due to the legitimate expectations that they create (*Louwage* 1974, para 12). If that is the case, the public body may not depart from the established policy, 'without giving the reasons which have led it to do so … ' (*Louwage* 1974, para 12).

As Paul Craig points out, 'guidelines, notices, communications and the like' officially approved by public bodies can give rise to legitimate expectations' (2018, 630). Such texts are not binding in the same way as formal laws, but official approval by the public bodies creates legitimate expectations that the very same bodies will not switch

their views, at least in the absence of 'convincing reasons' (Craig 2018, 630).[5] It should be added at this point that considerations regarding equal treatment may arise: in the absence of convincing reasons the public bodies cannot depart from an established policy with regard to a specific case (Craig 2018, 630).

The idea of legitimate expectations deriving from policy documents seems to be well-established in EU state aid law and EU competition law, where the Commission deals with a large number of cases (Craig 2018, 631). Applying these ideas in the domain of data protection certification, DPAs should not depart from their previous decision of embracing design specifications in a data protection certification scheme, in the absence of convincing reasons. Thus, controllers, who abide by specific standards laid down by certification requirements, can legitimately expect that these specified methods satisfy requirements approved by the very same authorities that will subsequently monitor their compliance. Moreover, they can legitimately expect that, as long as a particular method suffices for certain actors in the tech-industry, the DPAs will not arbitrarily switch their views in their own case.

One could argue that the official approval of certification criteria cannot have a self-binding effect on the approving DPA due to the phrasing of article 42(5) GDPR, according to which, 'certification … is without prejudice to the tasks and powers of the [competent authority]'. This provision clarifies that the existence of a certificate does not preclude the competent DPA from further investigating whether a certified party complies with the requirements of the certificate, as well as the GDPR in general.[6] In that sense, article 42 (5) clarifies that the DPAs are still able to proceed to a *factual assessment* of whether a data controller actually complies with the law. However, it does not follow from this provision that the DPAs may arbitrarily switch their views, about what it takes for a data controller to comply with the law.

Frankly, the standardised practices laid down in certification criteria are not a comprehensive guide to compliance by design, especially at this very early stage of development of data protection certification. However, the principle of legitimate expectations makes the officially approved measures reliable stepping stones towards effective implementation of data protection by design.

Even though general schemes can lay down precise statements (for example, the annual assessment of the personnel in GDPR-CARPA), the conclusion about legitimate expectations is particularly valuable in view of sector-specific certificates, which (as already shown) may lay down very precise specifications of measures of compliance by design. In that sense, reflection upon technical solutions in a particular domain can lead to very precise certification criteria in sector-specific schemes. That is because sector-specific schemes can identify which of the existing technical solutions sufficiently protect the data subject rights in their domain of application. When a data protection authority approves some technical standard, which is a product of such considerations, data controllers can get very reliable guidance as to which technical measures are deemed sufficient. As the example of the Age Check scheme shows, the authoritative guidance of certification criteria can reach as far as providing quantified benchmarks. The authoritative approval by the competent DPA and possibly by the EDPB makes the quantified values in certification criteria, reliable benchmarks for compliance by design.

Standards developed outside the GDPR framework

Unlike the officially approved certification requirements, other standards cannot create legitimate expectations, on the basis of the findings of the previous subsection, since they lack the official approval by the competent DPA. In that regard, the standards of the International Organisation for Standardisation (ISO) should be mentioned, as they are well-known and they are highly recognised world-wide (Lachaud 2020, 195). Especially, ISO/IEC 27701:2019 on security techniques in information management and ISO 31700:2023 on privacy by design are relevant.[7] However, they cannot be a source of authoritative guidance similarly to approved certification criteria because they lack the official approval by the competent DPA. Instead, ISO aims at laying down more globalised standards pertaining to privacy and data protection, and they do not describe how one can comply with the GDPR specifically (Lachaud 2020, 195).

This argument should not be understood as meaning that ISO standards are not pertinent to certification criteria of article 42 GDPR. Officially approved criteria may make references to ISO standards as best practices for bringing personal data processing into compliance with the GDPR's prerequisites. However, this task takes an extra step of explaining how the ISO standards can be used within the context of GDPR compliance. References to ISO standards are emerging in the domain of officially approved codes of conduct in accordance with article 40 GDPR.[8] In particular, the code of conduct of Cloud Infrastructure Services Providers in Europe (CISPE) mentions that when the cloud infrastructure service provider is doing risk management for the purposes of GDPR compliance, they should follow a methodology based on international industry standards, such as ISO/IEC 27005:2022 (CISPE 2021, 35).[9]

This practice can be potentially applied to certification criteria of article 42 GDPR, which may also include references to ISO standards. If that is the case, the drafters of the certification criteria should explain how such ISO requirements relate to GDPR compliance. However, once references to ISO standards become part of approved certification requirements, in accordance with article 42 GDPR, then they also offer authoritative guidance and may create legitimate expectations for data controllers.

The practical value of legitimate expectations deriving from certification criteria

A thought experiment can further illustrate the practical value of the protection of legitimate expectations deriving from the authoritative approval. Let us suppose that a data controller who is the developer of a digital application implements an age check solution which meets the reliability standards laid down in the form of certification requirements approved by the competent DPA. Let us also assume that the data controller in the example complies with an approved policy that requires annual assessment of their personnel, on matters of data protection compliance.

In case of an audit by the DPA, the data controller in the example has to prove compliance with the GDPR, in line with the principle of accountability (GDPR, art 5(2)). In that regard, a data protection certificate is a valuable asset in view of the principle of accountability. This idea directly derives from article 25(3) GDPR. However, the official approval of

the aforementioned compliance policies has an effect that goes beyond demonstration of compliance via certification.

If the data controller in the example proves (not necessarily by the means of a certificate) that they abide by officially approved standards, then the data protection authority cannot switch their views arbitrarily in the case beforehand. This does not mean that the DPA in our example cannot identify violations of article 25(1). Even though certification criteria can standardise certain technical and organisational safeguards, abidance by the certification criteria of any scheme does not guarantee compliance with article 25 (1) GDPR in all instances. The competent authority in the fictitious case might still deem that the controller *in casu* did not properly implement pseudonymisation measures and hence that there was a violation of article 25(1). What the authority cannot do, is to arbitrarily sanction the data control because the age check technology that they use is insufficient or because they had to assess the personnel biannually.

The idea of legitimate expectations deriving from certification criteria presented above does not leave the data subjects unprotected. As has been underlined so far, compliance with specific practices does not guarantee compliance with article 25(1) GDPR, and compliance with data protection by design does not guarantee compliance with data protection law in its totality. Hence, compliance with specific standardised practices by design does not mean that the data subjects are not able to exercise their rights. Moreover, data protection requirements found in data protection certification schemes are not binding for the Courts resolving civil disputes, as the certification criteria are not themselves laws, and the responsibility of the data controller is not reduced (GDPR, art 42(4)).

Specifications in certification criteria and the element of time

It should be mentioned at this point that, technological specifications in certification schemes face the danger of becoming obsolete. In that regard, article 25(1) clarifies that the identification of the necessary safeguards is not a one-off exercise. To the contrary, data controllers should be constantly updated in relation to new threats to data subjects and new technical and organisational solutions that offer a higher standard of protection (Koulierakis 2022, 44). One should not forget that article 25(1) was drafted in a vague manner in order to be able to deal with future technological challenges. Hence, new technologies may make the requirements of certification outdated, despite the authoritative approval by the competent DPA. For example, it is possible that the criteria of a certification scheme require that pseudonymisation under article 25(1) GDPR takes place with the use of an encryption method which was state of the art at some point in time but it becomes obsolete in the future.

In relation to these concerns the following points should be made in view of the legitimate expectations, deriving from certification schemes. First of all, the legitimate expectations of data controllers are not protected in an absolute way. As argued already, the principle of legitimate expectations obliges public authorities to provide reasons when they change their policies in a specific case. This conclusion also means that public authorities *may* change their views if there are good reasons for doing so. In the domain of technology regulation, technological innovation might constitute a convincing reason for DPAs to abstain from their previous action of embracing a particular measure of compliance with the obligation of data protection by design. In such a case, a DPA should

depart from its previous finding according to which abidance by specific requirements of approved schemes suffices for the purposes of article 25(1) GDPR or the GDPR in general.

It should be added that even if data protection certificates become obsolete, and the data processing does not fully comply with article 25(1) GDPR, the legitimate expectations of diligent controllers should not be disregarded. This is apparent in the case of certified controllers, since a data protection certificate is a reason for the DPA to impose a reduced fine, even if data controllers are in breach of the GDPR (article 83 (2)(j)). However, the effect of legitimate expectations deriving from certification criteria goes beyond the certified parties. In view of that, the legitimate expectations of data controllers should be respected as long as they follow standardised practices, even in the absence of a data protection certificate. For that reason, a DPA should first declare in some way that an officially approved standardised practice is obsolete, and then impose fines on data controllers. This derives from the principles found in the case of *Ferriere San Carlo*, where the ECJ ruled that when the Commission changes its established practice, they should first warn the stakeholders in 'good time' and then impose fines (1987, paras 11–12).

A theoretical example may clarify this point. Let us suppose that an officially approved certificate lays down an encryption method that becomes outdated at some point. In view of that, controllers who use the encryption method legitimately expect that this practice is reliable, regardless of whether they are certified or not. The position presented in this paper suggests that the DPA should not fine these controllers immediately for failing to effectively pseudonymise the personal data, irrespective of whether they are certified or not. Instead, the competent DPA should first declare that the encryption standard fails to meet the requirements of article 25(1), issue a reprimand or order the data controllers to bring the processing into compliance.[10]

One might argue that this understanding of the principle of legitimate expectations could be too restrictive for the data protection authorities in view of the fast pace of change in the domain of technology. However, the change of view of a DPA about certification requirements is a more agile procedure in comparison to law making. In that sense, the idea that certification requirements can offer guidance is a proposal that can more easily adjust to technological innovation, in comparison to the adoption of delegated acts, that the Commission originally envisaged, in view of data protection by design. For that reason, the idea of certification as guidance for data protection by design proposed in this paper, can be regarded as a middle ground between slow moving and inflexible law making, and complete absence of standardised practices of compliance by design.

Conclusion

The present paper started by arguing that article 25(1) is a vague provision, because it lacks references to specific technical and organisational safeguards. Additionally, the identification of the necessary safeguards is a product of a balancing exercise, which makes the identification of quantified measures very difficult. Existing use cases from the domain of data protection certification prove that certification requirements in officially approved schemes can lay down very specific technical and organisational measures, which can be used as guidance for data protection by design. Even though

guidance about compliance with GDPR obligations is not itself the aim of GDPR's certification framework, it can be a useful result, irrespective of what the drafters of a scheme pursue.

The guidance can reach as far as laying down quantified benchmarks. The present work argues that the approved criteria have an added value, which goes beyond certification, as an attestation of compliance. That is because they give strong indications to data controllers, about what it takes for one to comply with the obligation of data protection by design. Specifically, certification criteria may lay down standardised practices of organisational measures, and they can reach as far as providing the quantified benchmarks that technical measures should reach.

In relation to that conclusion, it should be clarified that sector-specific schemes can offer more specific guidance in relation to general ones, as the former are in a better position to take into account the technical and societal particularities of personal data processing, in a specific domain of activities. Thus, by taking into account the way competing rights and solutions relate in a particular domain of activities, a sector-specific scheme can reach as far as providing very precise benchmarks that the technical measure of article 25(1) should reach. However, as the study of GDPR-CARPA shows, even general certification schemes may lay down concrete policies of compliance measures.

Furthermore, data protection safeguards which have been adopted in the form of certification requirements have an authoritative character, even though certification criteria are not laws in a typical sense. The authority of officially approved certification criteria derives from the approval by the competent DPA and possibly by the EDPB. Approval by these bodies is a guarantee for the quality of data protection policies in the form of criteria, but as this paper suggests, there are further reasons for considering standardised policies in officially approved certification schemes. That is because the official approval by a DPA may create legitimate expectations for data controllers who abide by approved criteria. In that sense, certification criteria can be an authoritative source of guidance for data controllers, regardless of whether they are certified parties. Even though certification criteria cannot be a comprehensive guide to compliance with data protection by design, they can be reliable stepping stones towards the effective incorporation of GDPR principles into digital innovation. Meanwhile, authoritative guidance through certification requirements is more flexible in comparison to legally binding instruments, because data protection authorities are not prevented from changing their minds, in view of technological innovation.

However, the position that data protection certification requirements can function as authoritative guidance for data controllers requires a clarification. On the one hand, compliance by design comes first, as early as the stage of determining the means of processing. On the other hand, certification criteria can be seen as a way of identifying the effectiveness of the technical and organisational measures which are already in place. Even so, certification criteria can be a guiding tool, as data controllers could get a better understanding of what technical and organisational measures they should implement, at the moment of the determination of the means of processing, in order to achieve the standards, laid down in the certification criteria. In that sense, certification which is an ex post mechanism can offer valuable ex ante guidance. For these reasons, data protection lawyers as well as developers of digital applications that process personal

data should pay close attention to the growing corpus of officially approved certificates, in accordance with article 42 GDPR.

Notes

1. The present paper focuses on the certification scheme of articles 42–43 GDPR; data protection certification as an 'appropriate safeguard' for international transfers of personal data (GDPR, article 46(2)(f)) is not examined in the present paper. On the differentiation between data protection as an 'appropriate safeguard' and certification of GDPR compliance, see the opinion 25/2022 of the EDPB (2022b, 5).
2. According to article 4(7) GDPR, '"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data … '.
3. The data protection certification regime of articles 42–43 GDPR also relates to data processors. However, the present paper focuses on the added value of the certification regime of articles 42–43 GDPR, in relation to article 25 GDPR. Given that article 25(1) GDPR establishes an obligation for controllers, the present work only examines the data protection certification regime in relation to data controllers.
4. At the time of writing, the approved certification schemes within the EU are: GDPR-CARPA (CNPD 2022a; 2022b), EuroPriSe (EuroPriSe 2022a; 2022b), and Europrivacy ® (Europrivacy 2022). The Europrivacy® scheme has been approved by the EDPB, which lead to the creation of the first European Data Protection Seal (EDPB 2022c).
5. On the duty to provide reasons when EU bodies abstain from a general practice in a specific case see also *A v Commission* (1994, para 60) and the Opinion of AG Jacobs in *Austria v the Commission* (2000, para 35).
6. The (former) Court of First Instance of the EU has ruled that the principle of legitimate expectations does not affect the power of national authorities to reassess factual conclusions that were covered by the initial certification check (*Branco* 2005, paras 103–104).
7. ISO/IEC 27701:2019 is an extension to ISO/IEC 27001 (2022) and ISO/IEC 27002 (2022).
8. On the value of codes of conduct in view of legal certainty, see the work of Michal Koščík and Matěj Myška (2018).
9. The CISPE code of conduct has received approval by the EDPB (EDPB 2021).
10. On these powers of the DPAs, see articles 58(2)(a), 58(2)(b), and 58(2)(d) GDPR.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the KnowGraphs project, part of H2020 Marie Skłodowska-Curie Actions [Grant Number 860801].

References

Age Check. 2020. "Technical Requirements for Age Estimation Technologies (ACCS 1:2020)." www.accscheme.com/media/inahwyup/accs-1-2020-technical-requirements-for-age-estimation-technologies.pdf.

Age Check. 2021. "Technical Requirements for Age Appropriate Design for Information Society Services (ACCS 3: 2021)." ico.org.uk/for-organisations/certification-schemes-register/a-h.

Al-Sharieh, Saleh, Nikolaus Forgó, Jeanne Pia Mifsud Bonnici, Iheanyi Nwankwo, and Kai Wendt. 2018. "Securing the Person and Protecting the Data: The Requirement and Implementation of

Privacy by Design in Law Enforcement ICT Systems." In *Changing Communities, Changing Policing*, edited by Jeanne Pia Mifsud Bonnici, and Joseph Canatacci, 172–191. Austria: NWV Verlag.

Bygrave, Lee A. 2017. "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements." *Oslo Law Review* 4 (3): 105–120. https://doi.org/10.18261/issn.2387-3299-2017-02-03.

Bygrave, Lee A. 2020. "Article 25. Data Protection by Design and by Default." In *The EU General Data Protection Regulation: A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, 571–581. New York: Oxford University Press.

CISPE (Cloud Infrastructure Service Providers Europe). 2021. "Data Protection Code of Conduct for Cloud Infrastructure Service Providers." https://www.codeofconduct.cloud/the-code/.

CNPD (Commission Nationale pour la Protection des Données). 2022a. "GDPR Certified Assurance Report Based Processing Activities Certification Criteria (GDPR-CARPA)." Version 1. https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf.

CNPD (Commission Nationale pour la Protection des Données). 2022b. "The CNPD Adopts the Certification Mechanism 'GDPR-CARPA'." CNPD. Accessed June 5, 2023. https://cnpd.public.lu/en/actualites/national/2022/06/adpoption-gdpr-carpa.html.

Craig, Paul. 2018. *EU Administrative Law*. 3rd ed. New York: Oxford University Press.

EDPB (European Data Protection Board). 2019. "Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation." Version 3. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en.

EDPB (European Data Protection Board). 2020. "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2)." edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

EDPB (European Data Protection Board). 2021. "Opinion 17/2021 on the Draft Decision of the French Supervisory Authority Regarding the European Code of Conduct Submitted by CISPE." edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172021-draft-decision-french-supervisory_en.

EDPB (European Data Protection Board). 2022a. "Opinion 1/2022 on the Draft Decision of the Luxembourg Supervisory Authority Regarding the GDPR-CARPA Certification Criteria." edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en.

EDPB (European Data Protection Board). 2022b. "Opinion 25/2022 Regarding the EuroPriSe Certification Criteria for the Certification of Processing Operations by Processors." edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en.

EDPB (European Data Protection Board). 2022c. "Opinion 28/2022 on the Europrivacy Criteria of Certification Regarding Their Approval by the Board as European Data Protection Seal Pursuant to Article 42.5." edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europrivacy-criteria-certification_en.

EDPB (European Data Protection Board). 2022d. "The CNPD Adopts the Certification Mechanism GDPR-CARPA." EDPB. https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en.

EDPB (European Data Protection Board). 2023. "EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals." https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-adoption-edpb-opinions-regarding_en.

EU Commission. 2012. "Proposal for a Regulation of the Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." COM (2012) 11 Final.

EuroPriSe (European Privacy Seal). 2022a. "Criteria for the Certification of Processing Operations by Processors." Version 3. www.euprivacyseal.com/certification-schemes/scheme-for-processors.

EuroPriSe (European Privacy Seal). 2022b. "Europrise Cert Gmbh is the First Private Company in the EU With Certification Criteria Approved by the Competent Supervisory Authority." EuroPriSe. https://www.euprivacyseal.com/europrise-cert-gmbh-is-the-first-private-company-in-the-eu-with-certification-criteria-approved-by-the-competent-supervisory-authority/.

Europrivacy. 2022. "EuroPrivacy GDPR Core Criteria." https://community.europrivacy.com/europrivacy-gdpr-core-criteria/.

Garante per la Protezione dei Dati Personali. 2023. "Artificial Intelligence: Stop to ChatGPT by the Italian SA Personal Data Is Collected Unlawfully, No Age Verification System Is in Place for Children'." Garante per la Protezione dei Dati Personali. www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english.

Hildebrandt, Mireille. 2008. "Legal and Technological Normativity." *Techné: Research in Philosophy and Technology* 12 (3): 169–183. https://doi.org/10.5840/techne20081232.

Kamara, Irene, and Paul De Hert. 2018. "Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a Reformed Landscape." In *Privacy and Data Protection Seals*, edited by Rowena Rodrigues, and Vagelis Papakonstantinou, 7–34. The Hague, The Netherlands: Asser Press.

ISO (International Organization for Standardization). 2019. ISO/IEC 27701:2019".

ISO (International Organization for Standardization). 2022. "ISO/IEC 27001:2022." Latest Version.

ISO (International Organization for Standardization). 2022. "ISO/IEC 27002:2022." Latest Version.

ISO (International Organization for Standardization). 2022. "ISO/IEC 27005:2022".

ISO (International Organization for Standardization). 2023. "ISO 31700:2023".

Jasmontaite, Lina, Irene Kamara, Gabriela Zanfir-Fortuna, and Stefano Leucci. 2018. "Data Protection by Design and by Default:." *European Data Protection Law Review* 4 (2): 168–189. https://doi.org/10.21552/edpl/2018/2/7.

Koščík, Michal, and Matěj Myška. 2018. "Data Protection and Codes of Conduct in Collaborative Research." *International Review of Law, Computers & Technology* 32 (1): 141–154. https://doi.org/10.1080/13600869.2018.1423888.

Koulierakis, Efstratios. 2022. "The Challenge of Incorporating Legal Rules Into Digital Applications: A Theoretical Exploration of Article 25 GDPR." *ILLYRIUS International Scientific Review* 18 (1): 35–46.

Kuner, Christopher, Fred H. Cate, Christopher Millard, Dan Jerker, B. Svantesson, and Orla Lynskey. 2015. "Risk Management in Data Protection." *International Data Privacy Law* 5 (2): 95–98. https://doi.org/10.1093/idpl/ipv005.

Lachaud, Eric. 2020. "ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification." *European Data Protection Law Review* 6 (2): 194–210. https://doi.org/10.21552/edpl/2020/2/7.

Leenes, Ronald. 2019. "Regulating New Technologies in Time of Change." In *Regulating New Technologies in Uncertain Times*, edited by Leonie Reins. Berlin: Asser.

Michelakaki, Christina, and Sebastião Barros Vale. 2023. Unlocking Data Protection by Design and by Default: Lessons from Enforcement of Article 25 GDPR. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf.

Rodrigues, Rowena, David Barnard-Wills, Paul De Hert, and Vagelis Papakonstantinou. 2016. "The Future of Privacy Certification in Europe: An Exploration of Options Under Article 42 of the GDPR." *International Review of Law, Computers & Technology* 30 (2): 248–270. https://doi.org/10.1080/13600869.2016.1189737.

Senden, Linda. 2004. *Soft Law in European Community Law*. Portland, Oregon: Hart Publishing.

UK ICO (Information Commissioner's Office). n.d. "Age Appropriate Design Certification Scheme (AADCS)." ICO. Accessed September 11, 2023. https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-appropriate-design-certification-scheme-aadcs/.

Legislation

Regulation (EU). 2016/679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC: General Data Protection Regulation. Consolidated version. data.europa.eu/eli/reg/2016/679/2016-05-04.

Case law (in chronological order)

European Court of Justice

Judgement of 30 January. 1974. *Louwage*, C-148/73, ECLI:EU:C:1974:7.
Judgement of 21 September. 1983. *Milchkontor ao*, C-205/82, ECLI:EU:C:1983:233.
Judgement of 12 November. 1987. *Ferriere San Carlo*, C-344/85, ECLI:EU:C:1987:486.
Opinion of AG Cosmas delivered on 8 June. 1995. *Duff ao*, C-63/93, ECLI:EU:C:1995:170.
Opinion of AG Jacobs delivered on 13 July. 2000. *Austria v Commission*, C-99/98, ECLI:EU:C:2000:396.
Judgement of 13 March. 2008. *Vereniging Nationaal Overlegorgaan Sociale Werkvoorziening ao*, C-383/06, ECLI:EU:C:2008:165.

(Former) Court of First Instance

Judgement of 14 April. 1994. *A v Commission*, T-10/93, ECLI:EU:T:1994:39.
Judgement of 30 June. 2005. *Branco*, T-347/03, ECLI:EU:T:2005:265.