MAX VON GRAFENSTEIN

Specific GDPR certification schemes as rule, general schemes (and criteria) as exception

Comment on EDPB's Addendum to Guidelines 1/2018 on certification and identifying certification criteria per Articles 42 and 43 GDPR

(extended version 2)

HIIG DISCUSSION PAPER SERIES 2021-04

BACKGROUND INFO

This comment is based on the experiences and learnings from several research projects (being) conducted at the Alexander von Humboldt Institute for Internet and Society (HIIG) and the Einstein Center Digital Future (ECDF).

RELEVANT HIIG RESEARCH PROJECTS

Data Protection by Design in Smart Cities (2016-2018): Certification of data use

Data Protection as a Service (ongoing): Certification as competitive advantage

Data Governance: Finding Common Ground for Interdisciplinary Research (2019-2020)

Data and Society Interface (ongoing)

RELEVANT ECDF RESEARCH PROJECTS

FreeMove (2021-2023): Anonymisation and certification of movement data

WenDE (2020-2024): Certification of data processing in the building sector

AUTHOR INFO

Dr. Max von Grafenstein, LL.M., is attorney at Law at iRights.Law Berlin, founder of the academic spin-off Law & Innovation, full professor of the chair Digital Self-Determination at Einstein Center Digital Future and Head of Research The Governance of Data-Driven Innovation at Alexander von Humboldt Institute for Internet and Society.

CITATION

von Grafenstein, M. (2021). Specific GDPR certification schemes as rule, general schemes (and criteria) as exception: Comment on EDPB's Addendum to Guidelines 1/2018 on certification and identifying certification criteria per Articles 42 and 43 GDPR. HIIG Discussion Paper Series 2021-4. 19 pages. https://doi.org/10.5281/zenodo.4808841

LICENCE

CONTENTS

EXECUTIVE SUMMARY (extended version 2)

The ability of certification owners to set up general certification schemes alongside specific schemes is a fundamental design flaw in the interpretation of Articles 42 and 43 GDPR. General certification schemes open a glaring loophole for non-compliance with the law. To close this loophole, the EDPB makes a recognizable effort in its addendum, specifying further requirements for general certification schemes. However, these efforts are corrective measures as the fundamental design flaw continues to exist.

CONSEQUENCES OF GENERAL SCHEMES FOR MATTERS OF TRANSPARENCY AND COMPLIANCE:

- General certification schemes are black boxes that decrease transparency on how processing operations are legally assessed, and resultingly decrease consistent, EU-wide compliance with the GDPR. In the absence of concrete criteria,
    - authorities cannot check in advance how certification bodies apply the GDPR to a *specific* processing operation (Art. 42 sect. 5 and sect. 1 GDPR),
    - the publication of the criteria misses the mark, since the public is not able to form a picture of the *specific* interpretation either (Art. 43 sect. 6 and Art. 42 sect. 5 GDPR),
    - the coherence mechanism cannot apply to avoid inconsistencies in the EU-wide interpretation of the GDPR by certification bodies (Art. 63 GDPR).
- General certification schemes prevent the scaling of legal enforcement. They push the possibility of data protection supervision by authorities from the moment of approving the scheme (Art. 42 sect. 5 GDPR) to a moment after the certificate has been granted (Art. 43 sect. 5 GDPR).
    - Based on the approval of *specific* schemes, many certification bodies can certify innumerable processing operations; this leads to a scaling of law enforcement:
        - The authorities can suggest the EU-wide consistent and correct application of the law by default,
        - returning to a monitoring function by reactively checking the reasons for why the certificate has been granted.
    - If, by contrast, a certificate was issued on the basis of a general scheme, the authorities must now carry out, retrospectively, a full assessment for each individual case in which a certificate has been granted:
        - This leads back to the current overloads of the authorities.
        - In case of misapplication of the law, the authority can only react to the certificate already issued and the non-compliant processing operation already in progress (if the authority has the capacity to do so at all).
- For companies (esp. SMEs), general schemes are not a suitable way of dealing with the multitude of processing operations. Instead, a modularised system of specific certification schemes is a resource-saving means to reach this flexibility.

GENERAL CERTIFICATION SCHEMES CAUSE UNFAIR ECONOMIC DISADVANTAGES FOR COMPANIES TO BE CERTIFIED AND SPECIFIC SCHEME OWNERS:

- General certification schemes profit more from lower administrative costs in scheme approval than specific schemes do:
    - One general scheme can be applied to many different processing operations, while the competent authority has only to approve and charge the scheme once.
    - In contrast, owners of specific schemes must let authorities approve each single scheme per se, and pay corresponding fees accompanying each approval.
- General certification schemes lead to higher certification costs for companies being certified than those certified with specific schemes.
    - In practice, general schemes shift the efforts of specifying the certification criteria from the stage of creating the scheme to the stage where the scheme is applied. This is economically better for certification bodies, but worse for data controllers or processors who have to pay for the certification efforts.
    - Instead, specific schemes lead to economies of scale. The higher single cost involved in developing a specific scheme is offset by lower costs for its repeated application.
- However, general certification schemes profit from first market entry with increased brand reputation and market share, leaving behind companies with specific schemes disadvantaged by a more complex procedure of approval.

RECOMMENDATIONS:

- Specific certification schemes must be the rule, while general schemes and criteria can only be approved in exceptional cases. Such exceptional cases may be, in particular:
    - Data protection authorities grant certificates themselves. In this case, the lack of scaling law enforcement may be outweighed by the higher level of trust that arises when a certification is issued directly by a data protection authority.
    - Private scheme owners may be allowed to use general *criteria* when it is impossible to specify the GDPR provisions in advance, such as in the case of exploratory research processes. In such cases, however, scheme owners must
        - substantiate why it is impossible to specify the criteria and
        - accompany this lack of precision with procedural safeguards (e.g. by a monitoring data ethics board, by notifying the authority separately).
- Each certification scheme must target the purpose of a processing operation to demonstrate effective risk protection; targeting a processing operation indepently from its purpose is insufficient. In order for (components of) a processing operation to be certified on an individual basis, the risks associated with this single (component or) operation must be able to be evaluated and managed independently of other (components or) operations.
- **Legislators and the administration** should make it clear in all procedures in which they oblige the parties involved to adhere to a GDPR-certification scheme that this must be a *specific* scheme.

1 GENERAL CERTIFICATION SCHEMES CONTRADICT THE IDEA OF TRANSPARENT, EFFECTIVE, AND SCALABLE RISK PROTECTION

While the addendum raises and specifies many important and useful points, it perpetuates a major design flaw that the EDPB had already laid out in its Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of GDPR, namely, the possibility for certification owners to set up general certification schemes in addition to specific specification schemes. In the addendum, the EDPB makes a recognizable effort to close the loophole that opened up by this design flaw by specifying further requirements for such general schemes. However, these efforts are merely corrective measures: the fundamental design flaw continues to exist. The consequences are serious – the design flaw not only contradicts two key regulatory objectives, but will sooner or later marginalise more effective specific certification schemes in practice. To understand this assessment, it is necessary to have a closer look at the central function of certification schemes in environments which are highly prone to future uncertainties and covered by data protection law.

2 THE DECISIVE FUNCTION OF CERTIFICATION FOR THE GDPR

With the establishment of certification mechanisms, the EU legislator pursues two key objectives: increasing legal certainty and transparency and, on this basis, improving the implementation and enforcement of the law, in brief, compliance.[1] Conversely, effective certification mechanisms address two fundamental regulatory challenges: the significant lack of legal certainty and enforcement in practice. Both challenges are unavoidable consequences of the protection strategy a regulator usually chooses in a dynamic environment highly susceptible to change.[2] An example is the regulation of risks that the processing of personal data poses to the data subjects' fundamental rights. In fact, with its wide and cross-sectoral scope, the GDPR follows the conceptual logic used by most data protection (as well as

[1] See recital 100 GDPR.

[2] See Wolfgang Hoffmann-Riem, Saskia Fritzsche, Innovationsverantwortung – Zur Einleitung, 39, in: Martin Eifert, Wolfgang Hoffmann Riem (eds.), Innovations und Recht III - Innovationsverantwortung, 11-41, (Duncker & Humblot, 1st ed., 2009), pp. 259-262; Ivo Appel, Aufgaben und Verfahren der Innovationsfolgenabschätzung (Tasks and Procedures of the Innovation Impact Assessment), in: Martin Eifert, Wolfgang Hoffmann-Riem, Innovation und Recht III – Innovationsverantwortung, 147–181 (149) (Mohr Siebeck, 1st ed., 2009); cf., regarding technology regulation, Charles D. Raab and Paul De Hert, Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood, in: Roger Brownsword, Karen Yeung (eds.), Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes, 263–285 (2008); concerning cyber regulation, Andrew Murray, Conceptualising the Post-Regulatory (Cyber)state, in: Roger Brownsword, Karen Yeung (eds.), ibid., 287–316 (2008); further developed: Andrew Murray, The Regulation of Cyberspace – Control in the Online Environment In: Modern Law Review 70, (5) 879–883 (2007); and with respect to regulation per se, Robert Baldwin, Martin Cave, Martin Lodge, Understanding Regulation – Theory, Strategy and Practice, (2nd ed.) (2013); Claudio Franzius, Modalitäten und Wirkungsfaktoren der Steuerung durch Recht (Modes and Impact Factors for the Control through Law), § 4, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012); see also Martin Eifert, Regulierungsstrategien (Regulation Strategies), in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012).

modern privacy) approaches.[3] This logic follows the notion that the relevance of data, i.e. its risks, depends less on the nature of the data itself or its context of collection, but rather on which purpose or in which context the data is used for. A data protection approach which aims to defend data subjects against potential misuse of data for another purpose or in another context must necessarily encapsulate a cross-contextual scope.[4]

This approach has several consequences for lawmaking: first, it is evident that a legislator cannot foresee each detail of how personal data may be misused in one context or another, bringing forward the legislation issue on how exactly data subject can be protected against (potential) misuse. Second, a limited scope of knowledge requires the legislator to use broad legal terms and principles, i.e. a principle-based approach, rather than precise if-then-rules typically known as a rule-based approach. Broad legal terms and principles are therefore appropriate tools to regulate uncertain phenomena like processing risks; however, a principle-based approach provides fewer legal certainties and results in increased spending costs in case-by-case legal assessments to increase legal certainty. Likewise, a principle-based approach covers risks across different contexts, but risk overloading supervisory authorities in their ability to enforce the law. In fact, given the broad scope of the GDPR and the ongoing digitisation of our society, data protection authorities are far from being able to control the myriad of processing operations taking place in their areas of competence. To address the disadvantages of this risk-based, cross-contextual approach, legislators can complement this approach by establishing so-called co-regulation tools such as certification mechanisms (as well as codes of conduct and other similar mechanisms):

Certification schemes enable the data controller and/or processor to specify the broad legal terms and principles according to the particularities of their specific context. Specification typically occurs on the basis of the initiative or the proactive assistance of specialised scheme owners. Correspondingly, data protection authorities can delegate the enforcement of the law to certification bodies which are also specialised to the particularities of the context. To prevent such entities from misusing their specialized knowledge to the detriment of data subjects and the public, they must be audited by the competent supervisory authorities. This organization of oversight is the essential precondition of a co-regulation approach. In contrast, self-regulation lacks such supervisory mechanisms. Under a co-regulation approach, certification owners must have their scheme approved by a competent data protection authority.[5] Additionally, certification bodies must provide a positive certification decision which is made on the basis of such a scheme to the competent authority for review.[6] Only through these mechanisms, i.e. the proactive approval of the

[3] See Max von Grafenstein, Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design, forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990.

[4] See further references at Max von Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation), going to be published in EDPL 2/2021, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840116.

[5] See Art. 42 sect. 5 sent. 1 GDPR.

[6] See Art. 43 sect. 5 GDPR.

scheme and the reactive review of the specific certificate, can the supervisory authority prevent scheme owners and certification bodies from abusing their (in principle) superior context-specific knowledge. Likewise, this empowers the supervisory authority to prevent data controllers and processors from abusing the larger legal latitude that the risk-based approach grants. Additionally, the legislator can incentivize the use of these mechanisms by establishing certain legal privileges, for instance, some kind of legal presumption that a certified processing operation is deemed to be legally compliant.[7] Altogether, these mechanisms increase transparency and compliance. However, this idea only works in practice with certification schemes that are specific. General certification schemes, on the other hand, are inherently defiant in meeting these regulatory aims.

3 REGULATORY FAILURES OF GENERAL SCHEMES COMPARED TO SPECIFIC SCHEMES

Specific certification schemes concretize the broad legal terms and principles of the GDPR with respect to a specific processing operation. Making clear what is the exact matter at hand and how this matter is legally assessed in detail increases legal certainty for all parties, since the criteria must be made public.[8] Data controllers, data processors, data subjects, data protection authorities, and all other stakeholders have a legitimate interest in knowing how the law is implemented in a specific case (e.g. lawyers, authorities, data controllers and processors running similar processing operations, and even the public). If GDPR-certification schemes are to make this knowledge explicit to all interested parties, schemes must specify two elements: on one hand, they must disclose the specific risks of the data processing operation to be certified for the fundamental rights of the data subjects; on the other hand, certification schemes must explain how they concretize the respective applicable norms of the GDPR, so that every legal aspect, which is relevant to the certification decision and still disputed in the general legal debate, is made explicit and clearly decided. Only on this basis can the responsible data protection authority verify whether certification bodies apply the GDPR provisions in a way that meets the data protection authority's legal expectations. Only on this basis can the authorities initiate the coherence mechanism (Art. 63 et seqq. GDPR) if these legal questions, which have not yet been clarified in the legal debates, are disclosed. However, this also means that once the data protection authority has approved such a specific scheme, such a scheme may be scalable: certification bodies can multiply and certify innumerable processing operations. During the process of scaling up, the responsible data protection authority can suggest the EU-wide consistent and correct application of the law by default, returning to a monitoring function by reactively checking the reasons for why the certification body has granted the specific certificate to the certified controller or processor.

[7] See in particular Art. 24 sect. 3, Art. 25 sect. 3, Art. 46 sect. 2 lit. e) and f), Art. 83 sect. 2 lit. j) GDPR.

[8] See the requirement to publish the (specific) certification criteria in Art. 43 sect. 3 GDPR.

3.1 Black boxing each single case with general schemes

In contrast, general certification schemes create a black box which conceals the concrete implementation of law behind a certificate, seal, or mark professing to certify a processing operation as in compliance with GDPR. Since the certification criteria remain general, it is impossible to assess how the certification body verifies that the processing operation is GDPR compliant. This is not only true for the public, who can see the published criteria (according to Art. 43 sect. 5 GDPR) but cannot draw any conclusions about the concrete interpretation of the law because of their general nature. Not even the competent data protection authority has transparency on how the certification body assesses the risks and interprets the law in a specific case of a certain processing operation. The blackbox of general schemes therefore opens up a glaring loophole for both intentional and accidental misapplications of the law by certification bodies and, by extent, certified data controllers and processors.

3.2 Guidances would have to be as precise as specific schemes, rendering the concept of general schemes superfluous

Having opened a glaring loophole in its Guidelines 1/2018, the EDPB seems to have consciously tried to address this issue. At least, the board explicitly highlights the challenges for general certification schemes in containing criteria specific enough "to allow for coherent and consistent application of the same certification scheme within a [certification body] (in relation to different certifications / applicant) or between different [certification bodies]."[9] To avoid the risk of being too general, the EDPB recommends to "put a special emphasis on clarity of scope and purpose from the beginning about their scope and purpose" and that "a guidance note to auditors can play a key role".[10] It remains an open question as to whether the board is more concerned about the inconsistent application of a general scheme to various cases than possibilities for abuse and subversion of supervisory mechanisms. Perhaps the statement cited above is simply a very neutral way of expressing the problem. In any case, the EDPB's recommendation to fix this problem remains rather vague compared to what is necessary to appropriately address the issue at hand: in order to solve the problem caused by general certification schemes, a guidance must be as precise and mandatory as specific schemes. In addition, such a guidance would also have to specify to the same level of detail as in specific schemes every processing operation that is not excluded due to the broadness of the "general" scope. Of course, creating and applying this type of specific guidance would be so time-consuming that one might as well produce several specific schemes instead. Between general and specific schemes, cost might be a factor with respect to the administrative fees required for certification scheme approval (see in more detail below). However, apart from such a potential cost factor, there are no legal reasons that speak in favor of general schemes, but rather clear and serious reasons against them.

[9] See EDPB, Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment, adopted on 06 April 2021, cip. 34.

[10] See EDPB, Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment, adopted on 06 April 2021, cip. 34.

3.3 Specifying the "reasons" for granting a general certificate prevents the scaling of law enforcement

Besides the use of guidances, a second potential firewall against the potential abuse of general schemes are the "reasons" that a certification body must provide the competent authority for having granted or withdrawn a certificate.[11] These reasons must therefore be specific enough to allow the authority to assess, at least at this very least moment, the aforementioned aspects: what risks the certified processing operation poses to the data subjects' fundamental rights, how the certification body specifies the broad legal terms and principles, and by extent, what requirements the certification body places on the company being certified to implement the GDPR (in order to manage the risks effectively). However, even in the instance that a certification body precisely specifies the criteria for granting certification (i.e., the risks and concrete application of the law) and how the positive certification decision was agreed upon (i.e., on the basis of verification methods and results), at least one regulatory goal will not be met: law enforcement will not be able to scale. In fact, we return to a primary issue at hand before the implementation of the certification mechanisms. Competent data protection authorities will have to review every single processing operation themselves, or at the very least, the certification body's assessment of the facts and its interpretation of the law. To reiterate: under such overwhelming requirements, authorities will never be in a position to actually supervise the majority of processing operations for legal compliance within their scope of competence. Worse, one can imagine the organisational overload of the consistency mechanism if it were to be initiated on a case-by-case level; if applied correctly, the number of cases will be in the hundreds of thousands.

3.4 Jeopardizing the public trust in certification schemes and the GDPR as a whole

In sum, the recommendations given by the EDPB in its Addendum are only corrective measures: the loophole *per se* continues to exist. This means that as long as general schemes are allowed, further efforts of the authorities will focus on closing this loophole and pose an invitation to companies (i.e. data controllers and processors who want to be certified on the basis of a general scheme as well as the corresponding certification bodies) to attempt to slip through it. Potential consequences of this trajectory could involve scheme owners who provide only superficial guidance notes in the schemes, or certification bodies which fail to provide sufficiently detailed reasons for granting the certificate. Despite all efforts to apply corrective measures to the loophole, the approval of general certification schemes therefore remains inherently flawed by the design of general schemes themselves.

This design flaw will jeopardize the public trust in certification schemes *per se* and the GDPR as a whole. The reason for this is that GDPR-certificates signal legal compliance *approved* by public authorities because the certification scheme has been approved by these public authorities beforehand. The loss of trust in GDPR-certificates, as well as the GDPR as a whole, is inevitable when approved general schemes ultimately fail to safeguard the rights of data subjects – and this will happen far more often than in the case of specific certification programs (which can be specifically checked in advance for such misapplications).

[11] See Art. 43 sect. 5 GDPR.

While a certified data controller or processor is held responsible for such a violation according to Art. 42 sect. 4 GDPR, this provision does not prevent the loss of public trust in not only GDPR certificates *per se* but also in the application of the GDPR.

For these reasons, general specification schemes are especially inappropriate to situations that require a particularly high level of trust. One example are data sharing services and data altruism, two concepts that have recently come into public view in connection with the Proposal for an EU Data Governance Act (Art. 9 sect.1 lit. b and Art. 15). If data subjects willingly share their personal data via such sharing mechanisms, several requirements meeting the increased demand for trust must be met. A central precondition is that the purposes for which the data shall be shared are specific. (The sharing of personal data *per se* is not a sufficiently specified purpose, just as the "transfer to third parties" is not a sufficient purpose specification by which personal data may be transferred.)[12] Data sharing service providers that aim at facilitating this kind of sharing will therefore be required to come up with solutions compliant with the requirement of purpose specification.[13] Certification schemes used to enhance transparency and compliance of these sharing services must likewise be specific (see in more detail below at point V. The processing purpose as a prior reference point to specify the ToE of certification schemes) if they want to meet the high standard of trustworthiness intended by the Data Governance Act. The same logic applies to similar situations characterised by an increased demand for trustworthiness. For example, if Member States should provide additional legal grounds for the processing of personal data (e.g. according to Art. 6 sect. 1 lit. c and e, sect. 2) and require a GDPR certificate as a legal precondition for processing, this would equally require specific certification schemes to meet a heightened demand for trust. In all these cases, general certification schemes would never meet such increased standards for trust in data processing. The reasons for this have been demonstrated before.

3.5 Interims conclusion: General schemes and criteria only in exceptional cases

For these reasons, general certification schemes and, thus, criteria may be allowed in exceptional cases, only. For instance, the law foresees the possibility for data protection authorities to grant certificates themselves. In this case, the regulatory goal of scaling up enforcement of the GDPR does not apply. In such a scenario, only the first regulatory goal applies, i.e. the regulatory aim of increasing legal certainty. However, the drawback of losing one regulatory goal is outweighed by the higher level of trust that arises when a certification is issued directly by a data protection authority. Reasons for this higher level of trustworthiness range from an ascertained set of skills (in terms of knowledge as well as organisationally) to the requirement to apply the GDPR consistently (via Art. 63 et seqq.) to the absence of economic goals or constraints. Therefore it is reasonable to expect that data protection authorities may also create and use general schemes. However, it should be clear that general certification mechanisms are intrinsically unable to meet the second regulatory goal of making law enforcement scale.

[12] However, see such insufficiently specified purposes often used in current data protection policies.

[13] See Jürgen Kühling, Der datenschutzrechtliche Rahmen für Datentreuhänder, in ZfDR 1/2021, pp. 9 et seq .

Another exception in which even private scheme owners are allowed to use (at least) general *criteria* refers to scenarios where it is impossible to specify the GDPR provisions in advance. This is the case, for instance, in exploratory research processes where the controller or processor seeks to find out whether it can use certain personal data for a specific purpose, and if so, which ways this personal data may be used. In such open-ended research processes, the controller or processor cannot yet specify the concrete processing operation itself, and whether such an operation will make sense at all. Consequently, the controller or processor has limited insight on how they will apply the GDPR provisions to this process. However, in such a case, the scheme owner must proceed in two steps: first, the scheme owner must provide an envisioned processing situation (by defining the data it wants to use and stating which purpose) and provide in detail why the scheme owner cannot specify the law. Only then may the scheme owner skip the specification of the law to the later stage of certification. Second, the scheme owner must subsequently accompany this lack of precision with procedural safeguards: for instance, to call in a commission to guide the subsequent specification of the criteria, or alternatively, to notify the data protection authority separately (who may object to the concretisation ex-post in individual cases).[14]

4 ECONOMIC DISADVANTAGES OF GENERAL SCHEMES FOR SME AND OWNERS OF SPECIFIC SCHEMES

Economic reasons are another factor which pose significant disadvantages not only for owners of specific schemes but also for companies that want to be certified. Some owners of general schemes and certification bodies prefer general schemes to specific schemes since they can postpone the specification as long as possible, thus buying themselves (albeit only purported) room for maneuver. In practice, general schemes are additionally associated with the expectation that they will cause less effort and costs for the scheme owners. However, this expectation results from a misunderstanding of the flexibility of specific schemes and is at the expense of the data controllers or processors to be certified, especially in the case of small and medium-sized companies or the owners of specific schemes.

4.1 Modularised systems of specific schemes are more resource-efficient than general schemes

Further, for controllers and processors, general certification schemes are not a more suitable way of dealing with the multitude of processing operations than specific schemes. In order to be able to flexibly certify the multitude of operations, a modularised system of specific certification schemes that complement one another is more suitable instead. According to such a modular system, controllers or processors may choose the specific certification scheme that they find most relevant for their own IT system to start. Over time, additional schemes can be added if necessary. At first, this might be a specific certificate that addresses a „horizontal" processing operation underlying the whole IT business (e.g. a cloud service); later one or more „vertical" schemes addressing more specific business operations may be added. Such a system of specific

[14] See Max von Grafenstein, How to Build Data-Driven Innovation Projects at Large With Data Protection by Design: A Scientific-Legal Data Protection Impact Assessment With Respect to a Hypothetical Smart City Scenario in Berlin, pp. 81 et seqq., online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606140.

certification schemes may be comparable with the IT-Grundschutz-Profiles by the German Federal Office for Information Security (BSI), which modernises and modularises the IT-Grundschutz-Catalogue.[15] Further, comparable to a baseline scheme, such as the IoT scheme by the European Union Agency for Cybersecurity (ENISA),[16] controllers and processors may also build upon codes of conduct (and even Binding Corporate Rules), which cover certain processing sectors (or the horizontal processing operations of multinational companies), by adding specific certification schemes for particular processing operations.[17] Against the background of such complementary co-regulation mechanisms and, in particular, modularisable certification systems, general certification schemes are unnecessary. Worse, not only are general schemes unnecessary, but they decrease transparency and compliance, as has been previously shown.

4.2 Higher certification costs for companies being certified (and unfair competitive disadvantages for specific scheme owners)

Apart from that, general certification schemes are accompanied by a number of unfair competitive advantages for certification bodies and owners of general schemes and, vice versa, financial disadvantages for companies as well as owners of specific schemes. One such unfair economic advantage for general scheme owners is that in sum they are likely to pay less for getting a general scheme approved than owners of specific schemes. One general certification scheme can be applied to many different processing operations, while the competent authority has only to approve and charge the scheme once. In contrast, owners of specific schemes must let authorities approve each single scheme *per se*, and pay corresponding fees accompanying each approval. Even if the competent authorities may charge more for a general scheme because it might be bigger than a specific scheme – for instance, if the guidance notes are really as detailed as specific schemes and not limited to certain processing operations. However, as demonstrated, owners of general schemes will in principle try to avoid going into much detail; insofar as the authority does not insist on the required degree of detail, owners of general schemes are likely to pay less overall.

More important than the amount of the administrative fee of competent supervisory authorities is an additional economical advantage for the owner of general schemes. In practice, general schemes simply shift the efforts of specifying the certification criteria from the stage of creating the scheme to the stage where the scheme is applied. This is economically better for certification bodies, but worse for data controllers or processors awaiting certification: Each company usually has to pay the costs for going through the certification procedure. There are auditors and other parties involved in the auditing and certification decision-making process which require payment, typically on an hourly basis. If the certification process takes longer because these parties must specify the criteria and adapt them to the processing operation at hand, as is the case with general schemes, this is certainly beneficial for the

[15] See at https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html.

[16] See at https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.

[17] See Max von Grafenstein, How to Build Data-Driven Innovation Projects at Large With Data Protection by Design: A Scientific-Legal Data Protection Impact Assessment With Respect to a Hypothetical Smart City Scenario in Berlin, pp. 81 et seqq., online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606140.

certification body's coffers – but to the detriment of the company being certified. In contrast, applying a specific scheme creates less effort for the auditing and so on. Specific schemes therefore generate fewer costs for the companies being approved in the certification procedure, an outcome which likely benefits companies awaiting certification but for certification bodies poses decreased economic gain.

For the certification body, specific schemes may have an even worse financial effect when taking into account the revenue stream for the scheme owner. Typically, the certification body has to pay a license fee (for being allowed to apply the scheme) to the scheme owner: this is often carried out in the form of a certain percentage of the certification body's own revenue from doing the certification. So, while the certification body must exert less effort in applying a specific scheme and receive lower revenues, it must likely pay a higher licence fee to the scheme owner because of the higher costs to the scheme owner for creating the specific scheme. On a financial level, certification bodies will therefore prefer general schemes to specific schemes.

This financial logic may even apply to situations where the certification body and scheme owner are the same entity. In that case, one might think that the higher costs for the creation of the scheme and the lower costs for the certification ultimately balance each other out, since both costs are incurred within the same entity. Moreover, the higher single cost involved in developing a specific scheme would be offset by repeated lower costs for the application of the scheme. As a result, the costs for the company to be certified could even decrease. Theoretically, the pressure on costs could therefore even incentivize choosing specific schemes over general schemes (in favor of the companies that have to pay a lower price for being certified). However, beside the higher administrative costs that specific scheme owners are likely to bear (see above), there are a couple of other reasons that obstruct the *potential* competitive advantage of specific schemes.

4.3 Delayed market entry of specific schemes due to more complex approval procedures (and further disadvantages)

If both general and specific schemes were launched on the market at the same time, the provider of specific schemes could pursue this competitive cost benefit to their own and the certified companies' advantage. However, this is unlikely to be the case. Rather, general certification schemes may benefit from first market entry since they are (likely) faster than specific certification schemes approved by the competent authority. Underlying the difference in approval speed is the complexity involved in the approval procedure for specific schemes by the competent data protection authority. As outlined above, certification schemes must provide specific criteria to substantiate the broad legal terms and principles of GDPR in regards to each specific processing operation. Not only must the scheme owner substantiate the explicit characteristics of the processing operation, but the owner must also substantiate specific risks presented by said processing operation. Additionally, the scheme owner must also substantiate the respective applicable norms of the GDPR; to this effect, every aspect which is currently up for debate in the ongoing legal discussion and relevant to the certification decision must be made explicit and clearly decided according to one or another legal opinion. Moreover, the competent data protection authority has to initiate the consistency mechanism if the authority should find inconsistencies in how certain GDPR provisions are applied. Even

if there is a time limit set by law to bring the consistency mechanism to an end, the procedure for approving a specific scheme will take more time than the procedure for approving a general scheme, which likely conceals all these detailed legal questions. However, only in such a scenario can the competent data protection authority verify whether certification bodies apply the certification scheme in a way that meets the data protection authority's legal expectations in a EU-wide consistent manner. Thus, the degree of detail involved in the procedure for reviewing, discussing and approving the specific scheme is more complex than a general scheme; in a general scheme approval, these complexities are likely to remain largely untouched. Only when the certification body provides the responsible authority with the reasons behind granting a requested certificate is an explicit level of detail revealed. However, this degree of detail is achieved after the certification scheme has been approved, if it is to be achieved at all. Consequentially, general schemes are much more likely to be approved and enter the market faster than specific schemes. This leads to significant first market entry advantages, among which include a competitive edge on brand recognition, market share, and customer loyalty (given that certifications are typically granted for three years, Art. 42 sect. 7 GDPR).

In addition to delayed market entry, there are further competitive disadvantages for specific certification schemes. For example, specific certification schemes must make their knowledge publicly available: this includes, as previously highlighted, the specification of risks caused by the processing operation being certified, and the application of GDPR provisions to this operation (Art. 43 sect. 6 and Art. 42 sect. 5 GDPR). Competing certification bodies may use the specific criteria for designating the general scheme applied in their certification processes; in contrast, the publication of general criteria have little utility for the purpose of specification in GDPR. As such, general specification schemes create several competitive disadvantages for specific schemes, despite specific schemes offering more transparent, effective, and scalable risk protections.

5 THE PROCESSING PURPOSE AS A PRIOR REFERENCE POINT TO SPECIFY THE TOE OF CERTIFICATION SCHEMES

Regardless of whether or not general schemes should be prohibited, it is crucial to clarify that the specification of a ToE must always be made with respect to the purpose of a processing operation for the sake of effective risk protection. While the wording of Art. 42 sect. 1 GDPR refers to the term "processing operation" only, it is clear from the concept of data protection law (incl. the GDPR) that each processing operation of personal data follows a specified, explicit and legitimate purpose. Specification of the processing purpose is a central tenet of data protection laws, since the relevance of personal data is derived from the purpose in which that data is used. The EDPB issued a corresponding statement on the principle of purpose limitation in its Opinion 03/2013:

> "*Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations. As a prerequisite for other data quality requirements, purpose specification will determine the relevant data*

> *to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose/s.*"[18]

Conceptually, data protection laws protect data subjects against risks to their fundamental rights created by processing their personal data. In this framework, the specification of the processing purpose is *the* key indicator of which risks a planned processing operation may pose to the fundamental rights of the data subjects.[19] Thus, certification schemes for (one or more) processing operations must take the purpose of processing operations into account in order to effectively "enhance transparency and compliance with the [GDPR] Regulation".[20] This means that the target of evaluation of certification schemes must refer to processing operations that cause a risk that is specified in and of itself; correspondingly, a processing operation can only be certified independently of other operations if its risk is manageable independently of other operations.

This clarification is necessary as the addendum leaves the impression that processing operations may be certified regardless of the corresponding processing purpose and its respective risks. This impression is given by the examples that the EDPB sets for processing operations targeted by specific schemes: for instance, the "pseudonymization of personal data (...) or for a specific sector activity (example: data processing in stores)." As such, the pseudonymisation of personal data is not a processing operation that can be legally assessed in and of itself; rather, it is a technical-organisational measure intended to decrease the risk that a processing purpose poses. This also applies to an anonymisation of personal data in which the anonymisation process aims to exclude the actual processing operation from the scope of the law. Even in this context, the certification scheme must clarify for which underlying purpose the personal data shall be anonymised; this is to enable an assessment of the de-anonymisation risk (which ultimately depends on the underlying purpose) and, consequently, of whether the anonymisation of the data can be legally regarded as successful. Similarly, "data processing in stores" can be substantiated through a variety of different purposes, including payment at checkout, monitoring of employee performance, theft protection, in-store marketing, etc. Certification schemes must specify these purposes and the corresponding risks in order to effectively increase transparency and compliance.

6 CONCLUDING RECOMMENDATIONS

The ability of certification owners to set up "general certification schemes" alongside "specific certification schemes" is a fundamental design flaw in the interpretation of Articles 42 and 43 GDPR. General certification schemes open a glaring loophole for non-compliance with the law. To close this loophole, the EDPB makes a recognizable effort in its addendum, specifying further requirements for general

[18] EDPB, Opinion 03/2013 on purpose limitation (adopted 2013), pp. 11 and 12 .

[19] See Max von Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation), going to be published in EDPL 2/2021, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840116.

[20] See recital 100 GDPR.

certification schemes. However, these efforts are merely corrective measures as the fundamental design flaw continues to exist. The consequences of general schemes for matters of transparency and compliance are serious:

- General certification schemes are black boxes that decrease transparency on how processing operations are legally assessed, and resultingly decrease consistent, EU-wide compliance with the GDPR.
- General certification schemes prevent the scaling of legal enforcement. They push the possibility of data protection supervision by authorities from the moment of approving the scheme to a moment after the certificate has already been granted.
- For companies (esp. SMEs), general schemes are not a suitable way of dealing with the multitude of processing operations. Instead, a modularised system of specific certification schemes is a resource-saving means to reach this flexibility.

General certification schemes cause several economic disadvantages for companies that want to be certified and specific certification scheme owners:

- General certification schemes profit more from lower administrative costs in scheme approval than specific schemes do.
- General certification schemes lead to higher certification costs for companies being certified than those certified with specific schemes.
- General certification schemes profit from first market entry with increased brand reputation and market share, leaving behind companies with specific schemes disadvantaged by a more complex procedure of approval.

Recommendations:

- Specific certification schemes must be the rule, while general schemes and criteria can only be approved in exceptional cases.
- Each certification scheme must target the purpose of a processing operation to demonstrate effective risk protection; targeting a processing operation indepently from its purpose is insufficient. In order for (components of) a processing operation to be certified on an individual basis, the risks associated with this single (component or) operation must be able to be evaluated and managed independently of other (components or) operations.
- **Legislators and the administration should make it clear in all procedures in which they oblige the parties involved to adhere to a GDPR certification scheme that this must be a *specific* scheme.**

7 ADDENDUM ON THE DEMONSTRATED LEVEL OF COMPLIANCE BY CERTIFICATION SCHEMES

One last remark shall be added in this addendum, since the following comment falls outside the scope of this article discussing the pros and cons of general and specific certification schemes. However, for the purposes of ongoing discussion, it is important to nevertheless clarify one key issue that is often misunderstood in the debate on certificates. Recital 100 GDPR states that certification mechanisms shall help "to quickly assess the level of data protection". This statement seems to fall in line with the opinion of some scholars who assert that certificates could and even should signal a level of data protection level higher than what is required by law.

This assertion is based on a misunderstanding of certification mechanisms in the GDPR system. First, the main purpose of certification mechanisms is not intended to signal a higher level of protection than what is required by the law. Rather, certification mechanisms function first and foremost to increase compliance with a law that leaves a large room for maneuver in order to cover unknown future situations, namely risks; this occurs by specifying the broad legal terms and principles to the particularities of a specific processing operation. The specification of broad legal norms is the central function of certification mechanisms and the necessary complement to the regulatory risk approach of the GDPR; thus, it is not about signaling a higher level of protection than the law.

Second, there is in fact little to no room to provide for a higher level of protection than what is required by the law. The reason for this is that once a controller implements a more effective protection measure than what has been applied so far on the market, this constitutes the new state of the art which subsequently must be taken into account by all other controllers (see Art. 25 sect. 1 GDPR). Thus, there is only a limited time frame in which a controller applies for a higher protection level than the current standard. This dynamic reference to the constant development of more effective protection measures is the decisive regulatory function of the state of the art requirement.[21] However, monitoring the state of the art is one of the most challenging legal requirements, a challenge which can be appropriately addressed by specialised entities like scheme owners and certification bodies.

[21] See further references at Max von Grafenstein, Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design, forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing, online available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990.

REFERENCES

Appel, Ivo (2009): Aufgaben und Verfahren der Innovationsfolgenabschätzung (Tasks and Procedures of the Innovation Impact Assessment). In: Martin Eifert, Wolfgang Hoffmann-Riem (1st ed.), Innovation und Recht III Innovationsverantwortung, 149, 147–181.

Baldwin, Robert, Cave, Martin, Lodge, Martin (2013): Understanding Regulation – Theory, Strategy and Practice, (2nd ed.).

Eifert, Martin (2012): Regulierungsstrategien (Regulation Strategies). In: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (2nd ed.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation".

European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool.

Franzius, Claudio (2012): Modalitäten und Wirkungsfaktoren der Steuerung durch Recht (Modes and Impact Factors for the Control through Law), § 4. In: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (2nd ed.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation".

Hoffman-Riem, Wolfgang, Fritzsche, Saskia (2009): Innovationsverantwortung. In: Martin Eifert, Wolfgang Hoffmann Riem (1st ed.), Innovations und Recht III – Innovationsverantwortung, 39, 259-262.

Murray, Andrew (2007): The Regulation of Cyberspace – Control in the Online Environment. In: Modern Law Review, 70 (5), 879–883.

Murray, Andrew (2008): Conceptualising the Post-Regulatory (Cyber)state. In: Roger Brownsword, Karen Yeung, 287–316.

Raab, Charles D., De Hert, Paul (2008): Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood. In: Roger Brownsword, Karen Yeung, Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes, 263–285.

EDPB, Opinion 03/2013 on purpose limitation (adopted 2013), 11-12.

EDPB, Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) Certification criteria assessment (adopted on 06 April 2021) cip. 3.

Federal Office for Information Security: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html.

Kühling, Jürgen (2021): Der datenschutzrechtliche Rahmen für Datentreuhänder. In: ZfDR 1/2021, 9.

von Grafenstein, Max: Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design, forthcoming. In: González-Fuster, G., van Brakel, R. and P. De Hert, Research Handbook on Privacy and Data Protection Law, Values, Norms and Global Politics: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990.

von Grafenstein, Max (2020): How to Build Data-Driven Innovation Projects at Large With Data Protection by Design: A Scientific-Legal Data Protection Impact Assessment With Respect to a Hypothetical Smart City Scenario in Berlin, 81.: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3606140.

von Grafenstein, Max (2021): Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation), going to be published in EDPL 2/2021: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840116.