European Commission report on the General Data Protection Regulation

Feedback to the initiative “Report on the application of the General Data Protection Regulation”, pursuant to Article 97 of the GDPR

April 2020

About SRIW e.V. & SCOPE Europe sprl

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: **SRIW**) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self- and co-regulation. SRIW is also a monitoring body for data protection codes of conduct in Germany since 2011 and, yet, has successfully implemented and enforced two codes of conduct in the field of data protection. It further serves as a platform for the development, implementation, enforcement, and evaluation of various codes of conduct. SRIW has also actively contributed to the work of the Community of Practice for better self- and co-regulation during its mandate.

SCOPE Europe sprl / bvba (**SCOPE Europe**) is a subsidiary of SRIW. Located in Brussels, it aims to continue and complement the portfolio of SRIW in Europe and strives to become an accredited monitoring body under the European General Data Protection Regulation, pursuant to Article 41 GDPR. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers[1] and is engaged in other GDPR code of conduct initiatives. SRIW and SCOPE Europe (**the authors**) appreciate the opportunity to share our perspectives for the report on the application of the General Data Protection Regulation and, based on our experience, the following comments are made.

Selbstregulierung Informationswirtschaft e.V.
Albrechtstraße 10 B
10117 Berlin, Gemany

https://sriw.de

+49 (0)30 30878099-0

info@sriw.de

Amtsgericht Berlin Charlottenburg
Registernummer: VR 30983 B
USt-Nummer: DE301407624
Deutsche Bank AG
IBAN DE33 1007 0000 0550 0590 00

Chairman of the Executive Board
Dr. Claus-Dieter Ulmer

Managing Director
Jörn Wittmann

SCOPE Europe b.v.b.a/s.p.r.l.
Rue de la Science 14
1040 Brussels, Belgium

https://scope-europe.eu/
+32 2 609 5319
info@scope-europe.eu

Company Register: 0671.468.741
VAT: BE 0671.468.741.
ING Belgium
IBAN BE14 3631 6553 4883
SWIFT / BIC: BBRUBEBB

Managing Director
Jörn Wittmann

[1] https://eucoc.cloud/en/home/

Table of Contents

1 International transfers of personal data to non-EU countries

The free flow of data across borders is a cornerstone of the globalized world economy. The GDPR contributes for the necessity of movement of personal data globally, by introducing transfer mechanisms of personal data to third countries or international organisations in Chapter V GDPR. In the following, our feedback addresses two of these mechanisms: standard data protection clauses and codes of conduct.

1.1 Enhancing legal certainty for third country transfers

The standard contractual clauses for third country transfers introduced under the Directive 95/46/EC have not been updated to GDPR yet and are still in use, while currently under investigation by the European Court of Justice (ECJ) in the so-called "Schrems II" case. An update of the clauses by introducing standard data protection clauses pursuant to Art. 46.2 (c) GDPR would create much needed legal certainty for organisations that rely on pan-European data flows. In particular, clauses addressing the needs of processor-to-processor relationships are needed and currently missing, which is why SRIW/SCOPE Europe formed a consortium of different European and international companies from different sectors to develop key concepts that are necessary and worth considering for the overhaul of the clauses[2]. For instance, a key benefit for the implementation of standard data protection clauses should be a high-level of comprehensibility and accuracy, while avoiding redundancies or conflicts with other mandatory components for legally processing personal data, such as the Data Processing Agreement according to Art. 28 GDPR or the relevant technical and organizational measures. It is also important to note that the definitions of the current set of clauses as introduced under the Directive of data importer/exporter do not take into account a possible re-transfer of personal data into the EU by a sub-processor – which is a common scenario in today's processing activities of global enterprises.

Due to the high impact and complexity of this matter, the authors would appreciate the continuous dialogue between the European Commission and industries during the revision of the standard contractual clauses. As GDPR slightly modified the applicable terms, a consequent reference of standard contractual clauses (Art. 28 GDPR) as standardised processing agreements and standard data protection clauses (Art. 46 GDPR) as safeguard for third country transfers would be appreciated.

[2] The work of this industry consortium is available to the public to share perspectives on innovative concepts for standard data protection clauses in a processor-to-processor environment: https://scope-europe.eu/en/projects/standard-data-protection-clauses/

1.2 Robust oversight with codes of conduct

Besides the mentioned standard data protection clauses, approved codes of conduct pursuant to Art. 46.2 (e) in conjunction with Art. 40 GDPR can be a crucial, robust but innovation-friendly transfer mechanism. Codes of conduct can be developed by industries themselves, making it possible to introduce modern business practices and giving the flexibility of incorporating state-of-the-art technical and organizational measures while meeting all legal requirements as set out in Chapter V GDPR. One key advantage of codes of conduct is their thorough approval and oversight system: To achieve facilitated proof of GDPR compliance and become a safeguard for third country transfers, a code of conduct must be confirmed by the European Data Protection Board (EDPB) to provide appropriate safeguards and can be declared generally valid by the European Commission. Also, the compliance to a code must, in addition to the general oversight by data protection authorities, be supervised by an accredited, independent monitoring body.

The many benefits of an approved code of conduct for third country transfers make this a very attractive tool for the market and the competent authorities, that complements other existing data transfer mechanism. The respective guidelines by the EDPB are supposed to be published later in the year, which will be a crucial aspect for a successful and timely adoption for the first codes of conduct for third country transfers. Given the enormous benefits and impact, the authors would welcome timely adoptions of credible codes of conduct in this context, as these codes have the potential to ensure a cross-border data protection framework while ensuring a rigorous oversight. At the same time, codes of conduct for third country transfers can further contribute to the proper application of GDPR and ensure a high level of data protection for European citizens, even when their personal data is processed outside of the EU.

2 Codes of Conduct & Monitoring Bodies

The above mentioned sections outline the main argument to modernize standard contractual clauses and lists the key benefits of the adoption of codes of conduct for third country transfers. In the following, the authors want to focus more on general issues related to the implementation of codes of conduct and monitoring bodies, not only in the context of international data transfers.

In general, Art. 40 and 41 GDPR offer the possibility to implement the legal requirements of GDPR in a modern, innovation-enhancing way, while meeting all necessary data protection requirements. A significant market adoption of the tool as such will be possible, depending on the first approvals of codes of conduct in the near future. While the authors appreciate the many benefits in this context

given by the GDPR framework, our experience shows that particular provisions and mechanisms are not yet clear enough to be implemented or applied.

2.1 Codes of Conduct

2.1.1 Procedural aspects

Art. 40.4 GDPR introduces the requirement that a code "shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance". As per Art. 41.1 GDPR, the accreditation of this body is solely performed by the competent supervisory authority, unlike the approval of the code as such which, at least for all transnational codes, has to be endorsed by the EDPB. This leads to an ambiguity as it is not clear how to draw the line between incorporating the monitoring aspects that need to be covered in either the code (as per Art. 40 GDPR) or the accreditation process (as per Art. 41 GDPR). This could be particularly challenging for code owners that decide to mandate a monitoring body after developing the draft code as such.

Based on our experience, a practical solution to this is to include the general aspects how compliance is monitored in the code but leaving detailed and particularised procedures up to the accreditation of the monitoring body. A clarification on this aspect will surely simplify the development of codes of conduct in the future. Also, a code of conduct initiative can lose industry support and market momentum if the development is slowed down due to a search of a monitoring body during the drafting phase. Therefore, it should be possible to only include the general concepts for monitoring into the code, leaving the details up to accreditation of the monitoring body at a later stage. This could also enhance a competitive market, as the code owner could – if wished – even choose from several external monitoring bodies that raise their interest to oversee this particular code. Additionally, to the delay of selecting a suitable monitoring body already whilst drafting, a delay could result from the necessity of simultaneously developing detailed monitoring schemes. Though the authors recommend the support of a monitoring body during the drafting of a code of conduct – as this will significantly safeguard enforceability – the drafting of detailed monitoring schemes, including dedicated, code-specific procedures will lead to an unnecessary back-and-forth of drafting papers and consumption of resources.

Any approach distinguishing both procedures, whilst safeguarding that principles are always covered within a code of conduct already, will also strongly support the general aim of GDPR to foster a harmonised implementation of data protection law across the whole EU, since the accreditation of monitoring bodies solely performed by competent supervisory authorities will based on guidelines subject to the consistency mechanism within the EDPB, anyways. Especially codes of conduct applicable to

more than one member state will keep re-iterating EDPB alignment of core principles related to monitoring.

A second procedural aspect that creates some confusion in the market relates to Art. 64.3 GDPR, stating that an opinion of the EDPB on the approval of a code of conduct "shall be adopted within eight weeks". It is not clear how this deadline relates to the approval procedure for codes of conduct outlined in the EDPB Guidelines 1/2019[3]. Concretely, a clarification could be useful how exactly this eight week deadline is adopted and what deadlines are pending for other phases of the approval process. Nonetheless, the authors want to highlight, that those appreciate the streamlined procedures compared to those that were applicable under the Directive. Our comment is rather underpinning the relevance of predictability of procedures, also regarding timelines.

2.1.2 General validity

With regard to the general validity within the European Union, legal commentaries provide multiple interpretations of the exact implementation of Art. 40.9 GDPR. Such uncertainty can be hindering to some organisations to develop or join a code of conduct, as some interpretations claim that general valid codes of conduct will become mandatorily applicable to all who are within the original scope, regardless if one has voluntarily signed-up to such code. The authors consider this interpretation as not in line with the intention of the regulator and therefore, would welcome a clarification or amendment to increase clarity on the subject of general validity. This would further contribute to the adoption of codes of conduct in the future.

2.2 Monitoring Body

2.2.1 Mandatory obligation of monitoring and accessibility for SMEs

Art. 41.1 GDPR states that "the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out" by a monitoring body. Even though GDPR itself is clear that the oversight of a Code of conduct by a monitoring body is *mandatory* – e.g. as per Art. 40.4 GDPR or in accordance with the EDPB Guidelines 1/2019 – the use of the term "may" led to some confusion in the market in terms of the compulsory obligation of monitoring bodies.

One argument which was put forward in this context is that the obligation to have a monitoring body in place may overburden small and medium-sized companies (SMEs). Our experience suggests

[3] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf
Please find here our feedback to the EDPB consultation for the Guidelines 1/2019: https://scope-europe.eu/en/detail/news/scope-europe-submits-comments-on-edpb-code-of-conduct-guidelines/

otherwise: it is not the case that the monitoring overburdens code signatories that are SMEs. GDPR provides a sufficient degree of flexibility for the actual implementation of the monitoring, e.g. related to the actual monitoring scheme (frequency, type and scope of assessments). One example how the accessibility for SMEs is successfully reflected in the monitoring procedures is the EU Data Protection Code of Conduct for Cloud Service Providers, as reduced fees for SMEs and evidence-based conformity assessments make the code in particular interesting for smaller companies. At the same time, a large number of companies adhering to a code will, based on scalability of the overhead, lead to reduced compliance costs and thereby be a very attractive and implementable solution for SMEs, also compared to other compliance schemes. Scalability will even multiply for external monitoring bodies that apply for accreditation related to the monitoring of multiple codes of conduct. Also, it is worth pointing out that SMEs face implementation costs anyway in order to comply with GDPR. And in this context, a code of conduct – as providing particularized requirements – may help SMEs in saving resources to analyse and develop appropriate solutions to their needs.

2.2.2 Supervisory Authorities' competences related to the accreditation procedure

In daily operations, questions arose relating to the supervisory authority's competence for the accreditation of a monitoring body. Exchanges with supervisory authorities have proven that authorities are willing to resolve those questions pragmatically. Anyhow, to a certain extent, those solutions are pragmatic but still flawed with uncertainties – regarding both, predictability and legal sustainability and resistance in case decisions will be challenged. There seem to exist conflicts between business needs of monitoring bodies, their structure and means of establishment, competencies as provided by GDPR and limitations of national administrative law. Alongside some examples and actual current and past discussions, the authors will illustrate those concerns.

The most essential challenge will be if and to the extent there is a split in competency. This may occur frequently in cases where there will be an external monitoring body, a situation the authors strongly believe will be the default in future as this allows for scalability of providing monitoring services and thus will significantly decrease costs and eventually increase accessibility, see also 2.2.1. Also related to internal monitoring bodies situations are possible which may result into concerns as described above.

As an operating monitoring body for years, already under the Directive, the authors acknowledge and support the necessity that the accrediting supervisory authority needs resilient expertise related to the code of conduct the monitoring body applies for. Without code specific expertise – not in the subject matter as such but specifically related to the provisions and mechanisms of a code of conduct – it will be hardly possible to assess the appropriateness and feasibility of a monitoring body's

procedures. GDPR merely defines the competent supervisory authority for monitoring bodies by territorial means. Consequently, EDPB's guidelines allow for referring to the territorial competence of an intended monitoring body as criterion to determine the competency of a supervisory authority related to the approval of a code of conduct. Such a pragmatic approach is perfectly working at first sight; it will not prevent future obstacles, though, in cases a code and / or monitoring body will evolve.

Code-owners may have a need to change their appointed and accredited monitoring body over time; either by replacement or just by appointing additional monitoring bodies[4]. In other words, even if a split related to competencies can be prevented, it is likely that it will happen over time. GDPR's binary approach regarding the supervisory authority's competency related to the accreditation results into challenges and concerns resulting from national administrative law requirements. At least based on our exchange with key stakeholders there seem to be strong concerns that current requirements of GDPR cannot be (easily) addressed with current provisions of national administrative law. Some may even argue that member state's administrative law requirements can only be tackled by monitoring bodies establishing a national branch in each member state in which such monitoring body strives to provide its services; else supervisory authorities may not be legally enabled to apply GDPR requirements respectively perform, legally binding, their function as accrediting body. The latter, though, would conflict with European principles of freedom of establishment and freedom to provide services.

Consequently, it is suggested to carefully review Art. 41 GDPR regarding its provisions related to supervisory authorities' competence. Particularly, provisions related to the accreditation procedure are of concern. As of now, the authors recommend Art. 40 GDPR as starting point for future iterations, particularly its specific adoption of the consistency mechanism, Art. 63 GDPR. Current workarounds, that require simultaneous approval and accreditation will be unnecessarily burdensome and inflexible for both code-owners and monitoring bodies, see also 2.2.1.

2.2.3 Art. 41.6 (non-applicability for public authorities and bodies)

Art. 41.6 GDPR explicitly states, that "*This Article shall not apply to processing carried out by public authorities and bodies.*" As Art. 40 GDPR does not provide any equivalent, there seems consensus that also public authorities and bodies can draft codes of conduct respectively make themselves subject to codes of conduct drafted by others.

[4] EDPB guidelines explicitly state that it is possible – and even may be feasible in certain circumstances – to have multiple monitoring bodies for one code of conduct.

By keeping such possibilities accessible for public authorities and bodies, from our experience, GDPR has been drafted very wisely. Public authorities and bodies are seeking guidance how to apply GDPR, but often are - even more than industry - lacking resources to analyse and adapt processing activities, where necessary. Worsening, public authorities and bodies cannot rely – compared to private businesses – on the same information exchange among themselves to address legal uncertainties related to GDPR; not to mention complexities resulting from public procurement requirements. Approved common standards, therefore, seem to be desperately awaited; especially where public authorities and bodies are acting at the intersection of public duty and private business, such as power supply, public transport or even where data will be shared following open data principles.

Unfortunately, public authorities and bodies – at least to our experience – step back from using codes of conduct as it is unclear how the requirements of Art. 40.4 GDPR shall be met if Art. 41 GDPR is not applicable. This comes along with uncertainties, what is considered a public authority or body under Art. 41.6 GDPR, as usually public agencies are listed alongside, see e.g. Art. 4.7 to 4.10 GDPR.

Whilst many questions related to Art. 40 and 41 GDPR can be resolved by supervisory authorities and the EDPB, some questions require either clarification or amendments of the law itself. The latter seems to apply here. Thus, to better effectuate codes of conduct and eventually increase implementation of GDPR in general the following is suggested:

- The deletion of Art.41.6 GDPR would already enable the benefits for public authorities and bodies as described and therefore is the preferred suggestion.
- At least amending Art.41.6 GDPR to make it subject to the discretion of each member state if and to which extent Art. 41.6 GDPR shall apply to public authorities or bodies. For the avoidance of doubt: any approach, that results into a level playing field within Europe, is preferred; but the authors acknowledge that this relates to aspects of highest member state's concern, and therefore may require individual national variations based on the same principles.
    - Member states e.g. could define additional requirements for monitoring bodies pursuant Art. 41 GDPR if and to the extent they will be also monitoring public authorities or bodes (in general or related to specific authorities and bodies). This might be, that a monitoring body needs to be (also) subject to a national supervisory authority or to provide additional safeguards related to confidentiality; specific accreditation might also be possible, e.g. performed competent ministries, authorities or agencies provided such accreditation will only ensure additional requirements but does not undermine GDPR requirements and supervisory authorities independence.

- Limitations regarding the subject matter of a code of conduct do not appear necessary, as it is a public authority's or body's free choice to sign a voluntary mechanism like a code of conduct and thus is not required to make itself subject to any provisions it considers inappropriate.

- at least distinguish between monitoring and taking actions against public authorities and bodies. Principally, there seem to be no legal reason why public authorities or bodies must not declare themselves subject to contractual penalties. However, it is acknowledged that there might be other reasons that interfere, e.g. raison d'état. Still, it should be up to each member state if and to which extent monitoring bodies pursuant Art. 41 GDPR shall also be able to take actions against public authorities or bodies. One option might be that monitoring bodies pursuant Art. 41 GDPR are responsible for monitoring and complaint's management. This may also include the final judgement whether an actual infringement took place. However, the determination and enforcement of any action to be taken against public authorities or bodies shall be subject to any other (public) body competent; without any further member state law applicable, this is the supervisory authority competent.

3 Conclusion

This document outlines the perspectives of the authors with respect to the report on the application of the General Data Protection Regulation by the European Commission. On the topic of third country transfers of personal data, it is recommended to enhance legal certainty by introducing standard data protection clauses, particularly for processor-to-processor relationships. Also, the advantages of approved codes of conduct for third country transfers are discussed, a framework meeting market needs while creating benefits for competent authorities.

Regarding codes of conduct and monitoring bodies, the authors provide perspectives based on the extensive experience gathered. Clarifications on procedural aspects and the general validity as per Art. 40.9 GDPR would further benefit the market adoption of codes of conduct. For organizations acting as monitoring bodies, it would be helpful to better understand supervisory authorities' competences related to the accreditation procedure. Another relevant aspect to further enhance the adoption of codes of conduct could be the idea of amending Art. 41.6 GDPR to ease access for public bodies.

Executive Summary

This feedback to the initiative "Report on the application of the General Data Protection Regulation", pursuant to Article 97 of the GDPR, outlines the perspectives of SRIW e.V. & SCOPE Europe sprl. The authors focus mainly on the relevance of international transfers of personal data, particularly by standard data protection clauses and approved codes of conduct, and the general experience with the adoption of Art. 40, 41 GDPR.

- It is recommended to enhance legal certainty by introducing standard data protection clauses, particularly for processor-to-processor relationships
- It is recommended to start enabling codes of conduct as additional safeguard for third country transfers, as provided by GDPR.
- Regarding codes of conduct in general several needs of clarification are pinpointed and possible adaptions and enhancements, following practical needs and experience, are suggested.
- Regarding monitoring bodies in general several needs of clarification are pinpointed, with a focus on the relationship of Art. 40 and Art. 41 GDPR, especially related to the formal procedures of approval respectively accreditation.

selbstregulierung
informationswirtschaft e.V.

SCOPE
EUROPE

About SRIW e.V. & SCOPE Europe sprl

Self-Regulation Information Economy (German: Selbstregulierung Informationswirtschaft e.V. – short: SRIW) is a Berlin-based non-profit-organization that fosters and promotes data and consumer protection through self- and co-regulation. SRIW is also a monitoring body for data protection codes of conduct in Germany since 2011 and, yet, has successfully implemented and enforced two codes of conduct in the field of data protection. It further serves as a platform for the development, implementation, enforcement, and evaluation of various codes of conduct. SRIW has also actively contributed to the work of the Community of Practice for better self- and co-regulation during its mandate.

SCOPE Europe sprl / bvba (SCOPE Europe) is a subsidiary of SRIW. Located in Brussels, it aims to continue and complement the portfolio of SRIW in Europe and strives to become an accredited monitoring body under the European General Data Protection Regulation, pursuant to Article 41 GDPR. SCOPE Europe gathered expertise in levelling industry and data subject needs and interests to credible but also rigorous provisions and controls. SCOPE Europe also acts as monitoring body for the EU Data Protection Code of Conduct for Cloud Service Providers and is engaged in other GDPR code of conduct initiatives.