Computer & Communications Industry Association

Tech Advocacy Since 1972

CCIA response on the review of the application of the General Data Protection Regulation

General comments

CCIA firmly believes that the General Data Protection Regulation (GDPR) is a success and should not be reopened. The GDPR strikes the right balance between the protection of European citizens' personal data and enabling data-driven growth in Europe. The GDPR has extended well beyond the EEA, with companies across the world embracing the GDPR accountability model within their own organisation and across their supply chain.

However, we observe several deficiencies in the implementation and enforcement of the GDPR. They range from (1) a failure to implement all international data transfer instruments, (2) slow and unharmonised guidance for companies to comply with specific aspects of the Regulation, and (3) enforcement actions which undermine the One-Stop-Shop principle.

While some of them can be resolved through modest and practical improvements, others arise from structural deficiencies (local SAs) and fail to live up to the objectives and spirit of the GDPR.

The GDPR remains a living regulation and **CCIA is concerned that the enforcement status quo would, in the long term, bring severe discredit to what is otherwise a robust piece of legislation.**

CCIA appreciates the opportunity to submit our detailed observations and suggestions for improvements on the following aspects:

1. Data transfer instruments

Since the GDPR entered into force, most organisations transferring data outside the EEA have had 2 out of 5 transfer mechanisms at their disposal, namely Standard Contractual Clauses (SCCs) and adequacy decisions. There is a pressing need to develop other transfer mechanisms already contemplated in the GDPR, especially at a time when the legality of both the SCCs and Privacy Shield decisions are being questioned in court. Supervisory Authorities (SAs) have an important role to ensure that European and international organisations have the full range of data transfer instruments at their disposal and prevent any interruption of data flows between the EU and the rest of the world. These alternative mechanisms would complement SCCs and Privacy Shield, that we consider should be preserved.

Overall, there is a growing discrepancy between the urgency felt on the ground to develop additional transfer mechanisms, and the limited resources available to most SAs to conduct their work efficiently in this respect. At the same time, we are cognizant of the fact that SAs' lack of resources is a larger structural issue that affects other aspects of GDPR enforcement. We therefore urge Member States to allocate appropriate resources to their SA and ensure an efficient implementation of all aspects of the GDPR, including the review and approval of binding corporate rules (BCR), draft codes of conduct and certifications.

We provide additional observations on all data transfer instruments and recommendations for improvements further below.

Adequacy decisions

(a) General comments

CCIA was pleased to see the recent adoption of the Commission adequacy decision applicable to the transfers of personal data to Japan. We encourage the Commission to continue exploring opportunities for additional adequacy decisions in other third countries, in line with 2017 Communication on Exchanging and Protecting Personal Data in a Globalised World (COM(2017) 7).

(b) EU-UK personal data transfers

We take note of the provisions on cross-border data flows and personal data protection in the Draft text of the Agreement on the New Partnership with the United Kingdom (UKTF (2020) 14). CCIA appreciates the Commission's efforts to review the adequacy of the United Kingdom within the transition period. Consistent with the EU's approach to international data protection negotiations, we believe the **UK adequacy assessment should be performed and completed within this timeframe regardless of the outcome of the on-going trade negotiations** between the two parties. Lastly, we believe that the **adequacy review of the UK should be prioritised over any other adequacy assessment** given the strong data-driven economic relationship between the EU and the UK.

(c) EU-US Privacy Shield Framework

CCIA and our Members appreciate the Commission's continuous and rigorous review of the EU-US Privacy Shield Framework, and we remain committed to provide as much information as needed to help the Commission assess the functioning of this transatlantic framework. We believe that the degree of scrutiny brings additional credibility to the transfer of personal data to Privacy Shield certified organisations. For this reason, we encourage the Commission to replicate this review exercise to other adequate jurisdictions where it sees fit.

Standard Contractual Clauses

CCIA appreciates the Commission's commitment to review the existing decisions on SCCs. In doing so, **we encourage the Commission to reflect on the need to amend Decision 2016/2297 so that model clauses may be used by controllers established *outside* the European Union.** We note that Article 2 and Clauses 9 and 11 of Decision 206/2297 currently restrict the use of model clauses to 'data exporters'/controllers established in the EU. Yet, neither Article 46 nor any other provision of the GDPR preclude 'data exporters'/controllers established *outside* the Union from using standard contractual clauses to transfer data overseas.

We also encourage the Commission to adopt model clauses that may be used for the transfer of data from a processor to a sub-processor. As it stands, Decision 2016/2297 allows controllers only to export data outside the European Union. Yet in practice, processors often export data to sub-processors, for instance in the case of multi-cloud solutions and technology stacks[1]. While clause 11 does address sub-processing scenarios, the definitions of 'data exporter' and 'data importer' and the obligations and liability thereof are drafted with a controller-to-processor relationship in mind. New SCCs should address the specificities of processor-to-processor relationships.

Binding Corporate Rules

BCRs can be a useful alternative data transfer instrument that the GDPR has now codified.

However, the slow pace of the review and approval process significantly undermines the attractiveness and usefulness of this transfer mechanism. Two years after the entry into force of the GDPR, we note that the review and approval process take at least 12 months and up to 4 years depending on the competent SA involved. A common observation is a prolonged lack of feedback from SAs throughout the review and implementation process. We also note that the European Data Protection Board ('EDPB') also experiences significant delay in approving national decisions related to BCRs[2].

Only a limited number of organisations can afford to commit and dedicate resources on this transfer tool for such a long period of time. Most organisations continue using SCCs and/or Privacy Shield for transatlantic data transfers – two mechanisms currently under scrutiny by the Court of Justice of the EU. Companies and European citizens need legal certainty and the widespread adoption of BCRs could alleviate, at least partially, concerns arising from the uncertainty of other data transfer instruments.

In our view, the main reason for this backlog is the lack of appropriate staff, funding and other resources for most Sas (including authorities with prior experience with BCRs). Scarce resources require prioritisation of workload, and draft BCR are usually put at the bottom of the pile.

CCIA urges Member States to allocate appropriate resources to their SAs to ensure an efficient implementation of all aspects of the GDPR, including the review and approval of BCRs. **A maximum 12-month review process for SAs, and a 6-month review process for the EDPB should serve as clear indicators as to whether Member States are appropriately allocating resources to their SAs.**

---

1 This may also be relevant in the context of the European Commission Data Strategy, which seeks to establish 'federated cloud infrastructures';

2 In its contribution to the evaluation of the GDPR, the EDPB states that it had adopted 3 positive Opinions on national decisions related to BCRs. Meanwhile more than 40 BCRs are in the pipeline for approval, half of which could be expected to be approved by the end of 2020, the other half at an undisclosed date;

Codes of Conduct and Certifications

Similar to our comments on BCRs, we regret to see that the review and adoption process of Codes of Conduct is often too slow both at national and European level. We note that, two years after the GDPR became applicable, over 80 Codes of Conduct have been prepared but only a handful of national Codes of Conduct have been approved. At European level, the EDPB has not received a single Code of Conduct from SAs.

Yet, European and global organisations operating in Europe urgently need additional transfer mechanisms such as Codes of Conduct and certifications, especially at a time when the legality of both the SCC and Privacy Shield decisions are being questioned in court.

Once more, we believe that this is mainly the result of SAs' scarce resources and that codes of conduct typically feature at the bottom of their priority list. Going forward, **a maximum 12-month review process for SAs, and a 6-month review process for the EDPB should serve as clear indicators as to whether Member States are appropriately allocating resources to their SAs.**

Intra-EU transfers within the same group of undertakings

Although this consultation is about transfers outside the EU, we would like to take the opportunity to point to an intra-EU transfer problem that is the cause of a lot of burdensome paperwork to pan-European business operations.

Recital 48 GDPR rightly states: "Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data."

However, affiliates in different EU Member States that belong to the same group of undertakings are usually separate legal entities, and some SAs argue that the practice of centralising the processing of data for IT or business support services (e.g. employee and accounting) in a given Member State should be governed by a contract in the same way like with any third party outside that group of undertakings[3]. Failure to comply may trigger administrative fines.

Simplifying the contractual requirements for such intra-EU data transfers within the same group of undertakings through implementing guidelines that take into full consideration the spirit of Recital 48 would be very helpful to reduce administrative burden. These data sharing scenarios should be clearly treated differently from other exchanges within the group.

2. Consistency and cooperation mechanisms

CCIA observes two concerning trends that are already undermining the promise of data protection harmonisation in Europe. First, some SAs are circumventing the One-Stop-Shop (OSS) principle by directly engaging with entities with cross-border processing operations established in other Member States, and without having recourse to the cooperation mechanism under Article 60. Second, we observe a growing number of national guidance which contrast with interpretations and advice from other national SAs, and/or guidance from the EDPB. This is particularly worrisome when divergence emerge on fully harmonised provisions of the GDPR.

We provide additional observations and recommendations further below.

[3] See for instance the Conference of German Data Protection Authorities' guidance on Article 28, available on https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (December 2018)

One-Stop-Shop at risk

The OSS mechanism is a core principle of the GDPR that seeks to harmonise the fractured nature of data protection enforcement across Europe under the 1995 Directive, particularly for entities involved in cross-border processing operations. CCIA fully supports previous Commission statements confirming the OSS rules and their alignment with the EU's single market objectives[4]. This gives businesses the "certainty that they only need to deal with one SA for their cross-border processing activities leading to savings estimated at EUR 2.3 billion per year."

However, over the past 2 years, we have observed attempts by SAs to circumvent OSS mechanism and seek to exert jurisdiction on organisations whose main establishment is located in a different Member State. Local oversight measures range from information requests to infringement procedures and are often justified on the basis of novel interpretations of the GDPR, most notably an isolated reading of Article 58(5) and a narrow understanding of the concept of 'main establishment'.

We recall that the only derogation to the OSS is if a complaint or a possible infringement "relates *only* to an establishment in [the] Member State [of the Supervisory Authority] or substantially affects data subject *only* in [this] Member State."[5] Yet, most entities operating in multiple Member States define the purpose and means of processing *uniformly* across all relevant jurisdictions in the EU. In these circumstances, an SA cannot derogate from the OSS mechanism since the processing will always have an EU-wide dimension. We note that the OSS rules extend to all relevant powers of a lead SA in cross-border processing activities, including recourse to courts.

By circumventing the OSS, SAs fall short of their obligation to "contribute to the consistent application of [the GDPR] throughout the Union", including to "cooperate with each other and the Commission in accordance with Chapter VII" in cross-border cases.[6] Above all, disregarding the OSS rules contradict the main purpose of the GDPR reform, namely to achieve harmonised and consistent application of data protection rules in Europe.

Lastly, from a company perspective, such practices ultimately create risks of conflicting injunctions and remedies across the EU, could amount to double jeopardy, and ignore the significant amount of resources companies invest into building a constructive relationship with their lead SA. This is detrimental to business certainty and investment in Europe.

For all these reasons, **we encourage the Commission to strongly reaffirm the rules and obligations of the OSS and the cooperation and consistency mechanism in its June GDPR Review Report**. In doing so, SAs should be encouraged to actively participate in the decision-making process via the cooperation procedures rather than bypassing the rules by initiating their own proceedings.

We also invite the Commission and the EDPB to consider setting up a common repository of lead SAs for companies with cross-border processing operations for which they are responsible for. As this repository grows overtime, this could be a practical step to help SAs identify which companies they can directly engage with or which SA they should reach out to in the context of a cooperation procedure.

---

4 See European Commission GDPR FAQ on companies processing data in several Member States; and Joint Statement on the final adoption of the new EU rules for personal data protection (2016);

5 See Article 56(2) GDPR;

6 See Article 51(2) GDPR;

Discrepancies between national guidance and practices on harmonized data protection rules

We observe a growing number of national guidance which contrast with interpretations and advice from other national SAs, and/or guidance from the EDPB. This is particularly worrisome when divergence emerges on fully harmonised provisions of the GDPR.

While guidelines are non-binding, they are used as a checklist by SAs during their investigation and their content is often reflected in national infringement decisions. Guidelines also remain important tools for companies in practice as they continuously seek to comply with their obligations.

For instance, we observe significant divergence between the French[7], German[8], Dutch[9], UK[10], Spanish[11], Irish[12] and EDPB guidance over the processing of personal data retrieved from end user devices ("cookies"), ranging from consent exemption for analytic cookies and lawful grounds for subsequent processing, to information notice and cookie walls.

Another example is the lack of clear and harmonised guidance on the legal grounds to process personal data (Article 6 of the GDPR). In some cases, national guidance even conflicts with GDPR and the EDPB guidance. This is for instance the case with the Dutch SA's opinion on legitimate interest[13], which unlike the Article 29 Working Party guidelines, considerably restricts the range of interests that can be considered legitimate. The Dutch authority have already acted upon its interpretation in a recent decision[14], and this difference is likely to lead to different outcomes in the Netherlands than elsewhere in the European Union.

Lastly, procedures on sanctions also deserve far greater harmonisation across the EU. Today, most SAs corrective decisions or administrative fines are generally opaque and fail to demonstrate adequate due process and a transparent methodology. We believe the EDPB opinion on sanctions[15] should be further complemented by common minimum guidance on: (a) the appropriate safeguards during investigative and corrective proceedings, including the public disclosure of decisions, (b) the methodology determining when corrective sanctions are sufficient to address an infringement or if a fine should be levied on controllers and/or processors, and (c) a clear process to assess the amount of a proportionate and dissuasive fine in the event corrective sanctions do not sufficiently address the gravity of the infringement.

Discrepancies in guidance, coupled with opaque sanction procedural rules and the fact that potentially concerned SAs sometimes take on the role of lead authority (as described in the previous section), bring significant legal uncertainty and undue liability exposure for controllers, particularly those with cross-border operations.

While we respect the independence of SAs, we believe that the exercise of independent oversight functions should not be detrimental to the regulatory and enforcement harmonisation of the data protection framework in Europe.

---

7 Available on https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-de-nouvelles-lignes-directrices
8 Available on https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
9 Available on https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies
10 Available on https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf
11 Available on https://www.aepd.es/sites/default/files/2019-12/guia-cookies_1.pdf
12 Available on https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190612%20Guidance%20on%20Cookies%20and%20Similar%20Technologies.pdf
13 See the Dutch DPA 2019 guidance available on https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf
14 See the Autoriteit Persoonsgegevens's decision of 3 March 2020 against the Royal Dutch Tennis Association available on https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens
15 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 17/EN WP 253

To this end, **we invite the Commission to strongly encourage SAs to restrict their own guidance to data protection rules where Member States are explicitly allowed to legislate where GDPR permits.** At the same time, **more resources should be diverted to the drafting of practical and detailed guidance at the level of the EDPB**, as well as the dissemination of such guidance at national level. **The EDPB, acting as the guardian of GDPR harmonisation, should also set out clearer and more transparent internal rules.** Without prejudice to the confidentiality of sensitive commercial information, this should include better transparency on mandates, information on which SAs are in charge of drafting guidance, structures of the working groups, timelines for adoption of documents, improvement of the website of the EDPB to make information more easily accessible, publication of all official correspondence, and minutes and agenda of each meeting.

###

For further information, please contact Alexandre Roure, Senior Manager, Public Policy at aroure@ccianet.org.