Call for Evidence – Feedback

Report on General Data Protection Regulation

February 2024

The Computer & Communications Industry Association (CCIA Europe) welcomes the opportunity to provide feedback on the General Data Protection Regulation (GDPR) and its application, six years after the rules entered into effect.

For the GDPR to continue acting as a landmark horizontal framework, certain adjustments are needed. These could be introduced in the form of guidance on, or further harmonisation of, implementation and enforcement. Below you will find CCIA Europe's main reflections and recommendations regarding the GDPR's application and possible follow-up actions.

I. Continue ensuring unhindered, safe data flows

CCIA Europe supports the European Commission's efforts on adequacy frameworks, as well as standard contractual clauses, but would welcome further adequacy decisions to the extent possible as well as more proportionality when it comes to guidelines that have been developed.

Recommendations:

1. Adopt more adequacy decisions for jurisdictions meeting appropriate standards
2. Pay attention to tension between data protection and need for security
3. Ensure proportionality in guidelines developed by the EDPB

II. Respect the different legal bases for processing of data

The GDPR sets out a range of legal bases for processing of personal data. While each basis has to meet certain conditions, there should be no hierarchy between them.

Recommendations:

4. Avoid a restrictive interpretation of the different legal bases
5. Make consent work in practice

III. Guarantee harmonised implementation

The GDPR created a new architecture for the protection of personal data which needs to be adequately and uniformly implemented and enforced across the board.

Recommendations:

6. Ensure coherent implementation of the GDPR across all EU legislation
7. Strengthen the One-Stop-Shop mechanism
8. Avoid fragmentation in Member State implementation

Introduction

Since its entry into force, the General Data Protection Regulation (GDPR) has had a tremendous impact on the way organisations across the European Union gather, use, and store personal data. It has set the standard for higher protection of personal data worldwide, with many companies adapting their global data protection policies in response. The GDPR has brought a number of benefits, including an increase in accountability and transparency on how private and public organisations collect, process, and use personal data. It also led to an increased awareness of data subjects about their rights, paired with a higher investment in data protection by companies complying with the rules.

Nevertheless, organisations also face a number of challenges resulting from the GDPR, including an increased complexity with regards to the legislative framework and its application, the cost incurred by companies of all sizes to comply with the rules, as well as uncertainty with regard to the interpretation and enforcement of GDPR, both at Member State and European level. While welcoming the new proposed rules on GDPR enforcement as a complement to the existing data protection framework, CCIA Europe believes this proposal falls short of addressing important enforcement deficiencies we have observed since the entry into application of the GDPR.

After six years, it is necessary to take stock of these rules and how they have been applied. CCIA Europe welcomes the opportunity to reflect upon the application of the GDPR and would like to respectfully offer the following recommendations.

I. Continue ensuring unhindered, safe data flows

CCIA Europe supports the European Commission's efforts on adequacy frameworks, as well as standard contractual clauses, but would welcome further adequacy decisions to the extent possible as well as more proportionality when it comes to guidelines that have been developed.

1. Adopt more adequacy decisions for jurisdictions meeting appropriate standards

The GDPR introduced a number of helpful novelties for data transfers, codifying binding corporate rules and introducing certifications and codes of conducts for companies that seek to transfer data outside of Europe. However, these haven't been used as much as they could have. Organisations based in Europe still primarily rely on standard contractual clauses (SCCs) and adequacy decisions.

The European Commission has issued a low trickle of adequacy decisions throughout the past years, the last one on Japan in 2019.[1] Countries across the world are increasingly adopting laws establishing a safer environment for the treatment of personal data and guaranteeing appropriate standards for transfers of data. Consistent with the Council's

[1] European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

position on the application of GDPR,[2] further adequacy decisions and more flexibility as regards the mechanisms for international data transfers would facilitate transfers across our EU borders and create more legal certainty for a great number of businesses.[3]

In an era where significant economic value derives from unencumbered personal data flows,[4] it is necessary for the Commission to work together and align with other global actors in order to develop stronger interoperability between data flow systems in the European Union and other third countries.

2. Pay attention to tension between data protection and need for security

The importance of cross-border data transfers cannot be understated. However, in recent years, CCIA Europe's Members have experienced an increased tendency among EU regulators to view localisation as a way to protect personal data originating in the European Union.[5] This trend could limit businesses' ability to deploy state-of-the-art security threat detection and mitigation measures that rely on cross-border data transfers, thereby undermining industry's efforts to ensure the integrity of EU personal data. This would also contradict the obligation under Article 32 of the GDPR which mandates controllers and processors to take "into account the state of the art" and to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk". The tendency to increasingly push for the localisation of data also threatens information sharing among different industry players, as well as between those players and government agencies for security purposes.

Moreover, when it comes to international data flows, the treatment of IP addresses as personal data has also become problematic, as this treatment makes them subject to GDPR rules for data transfers. With IP addresses increasingly being treated as personal data, the GDPR would apply to those IP addresses ostensibly linked to EU residents and these would not be able to be processed in third countries with no adequacy decision. The unrestricted flow of IP addresses is crucial, both for the global functioning of the internet and to ensure advanced cybersecurity applications that depend on IP addresses and additional metadata sourced globally.

---

[2] Council position and findings on the application of the General Data Protection Regulation (GDPR): https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/en/pdf

[3] More information on ensuring secure data transfers can be found in CCIA's comments to the European Commission and the EDPB on Ensuring Data Transfers post 'Schrems II': https://ccianet.org/wp-content/uploads/2020/10/2020-10-27-CCIA-Comments-to-European-Commission-and-EDPB-on-Ensuring-Data-Transfers-post-Schrems-II.pdf

[4] Economic Value of Data Flows, by Tech4i2 and IPSOS for DG CONNECT, 2024: https://op.europa.eu/en/publication-detail/-/publication/7e31cf37-b036-11ee-b164-01aa75ed71a1/language-en; The economic impact of cross-border data flows, Frontier Economics, 2021: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf

[5] A hard data localisation requirement features in various drafts of the upcoming EU Certification Scheme for Cloud Services (EUCS). The EDPB supports the introduction of this requirement: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-enisa-regarding-european-cybersecurity_en; Article 27 of the Data Act also creates a separate regime for non-personal data transfers for cloud services providers subject to third party countries' data access requests, based on IP protection afforded in third countries. Because cloud providers cannot distinguish personal from non-personal data, an enforcement decision suspending the flow of non-personal data would necessarily affect personal data, and potentially collide with adequacy decisions, SCCs or other transfer tools under GDPR.

CCIA Europe would therefore welcome additional guidance clarifying that IP addresses should not be considered as personal data when they cannot be linked to a real person.[6] Further, the implementation of the GDPR should take account of the added security benefits that can stem from cross-border data processing. It should also be further clarified that personal data processed outside of the EU for cybersecurity purposes is to be exempted from the GDPR restrictions applicable to international data transfers.

3. Ensure proportionality in guidelines developed by the EDPB

The GDPR established the European Data Protection Board (EDPB) and empowered it to issue guidance for the application of different provisions in the data protection framework.

CCIA Europe has noted how, in recent years, some of the guidance provided by the EDPB fails to strike the right balance between the protection of personal data and the encouragement for businesses in the European Union to innovate. One clear example can be found in the EDPB Recommendations 01/2020,[7] which impose an excessive burden on businesses and deviate from the GDPR's risk-based approach to data protection. The Recommendations effectively prohibit most data transfers outside the European Economic Area (EEA), causing considerable economic and social harm without providing any commensurate benefits for the protection of European citizens' data[8].

Another example are the Guidelines adopted by the EDPB in May 2023 on the calculation of administrative fines, which do not necessarily take into account the principle of proportionality but rather focus on the need to establish GDPR fines that are dissuasive and effective.[9] To avoid the EDPB's guidance exceeding the limits of its remit, the European Commission should establish clear limits on the extent of the Board's guidance and define which topics it should cover.

II. Respect the different legal bases for processing of data

The GDPR sets out a range of legal bases for processing of personal data. While each basis has to meet certain conditions, there should be no hierarchy between them.

4. Avoid a restrictive interpretation of the different legal bases

While a number of legal bases to process personal data exist, CCIA Europe notes that since the application of the GDPR, regulators, courts, and lawmakers are increasingly relying on

[6] CJEU Case C-582/14 concludes that dynamic IP addresses constitute personal data only if the processor of the IP address is able to link the IP address to an individual: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582.
[7] Recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
[8] More information can be found in CCIA's comments on the draft EDPB Recommendations on supplementary measures: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/12-21-2020_-_ccia_response_to_the_edpb_on_schrems_ii_guidelines.pdf
[9] Guidelines 04/2022 on the calculation of administrative fines under the GDPR: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

consent as the preferred ground for data processing, while considerably restricting 'contract' and 'legitimate interest' to a limited number of scenarios.

The GDPR is clear about the fact that there is no hierarchy between different grounds. If we focus on the three most common bases for data processing, we can see differences in their application, namely:

When it comes to a contract as the legal basis, Data Protection Authorities (DPAs) have traditionally taken a restrictive approach with regards to what constitutes 'necessary' data processing.[10] This approach fails to take into consideration the transactional nature of contracts, the protection afforded under civil law (e.g. safeguards to ensure fairness and to protect against information asymmetry), and the extent to which contracts may fulfil the exercise of other fundamental rights, including individuals' freedom to enter into contractual relationships or the freedom to conduct a business.[11]

In the case of legitimate interest, privacy cannot be used as the only absolute consideration. Other user interests should also play into the equation, including economic interests as well as interests by third parties.

Moreover, consent is not always the most suitable legal basis. The iteration of consent places an unfair burden on the data subject, who – despite each and every controller's best efforts in providing clear, succinct information and actionable choice – will most likely prefer to 'click away' consent prompts. Furthermore, requesting consent from the data subject tends to presume that data protection is an absolute right, when it should actually always be weighed against other fundamental rights.

5. Make consent work in practice

The GDPR introduced a framework for obtaining and managing consent for the processing of personal data. However, during the past six years the regulatory framework has provided a lack of clarity on the applicability of the different legal bases, which has led to ongoing discussions among both regulators and policymakers.

While consent is increasingly becoming the preferred legal basis for lawmakers, regulators and courts, CCIA Europe considers that this approach does not properly take into account the limits of consent, nor the increasing fatigue that consumers face around such an option. This over-reliance on consent also dismisses the benefits that alternative legal bases might have both for individuals and controllers.

In order to effectively implement consent in practice, the Commission should recognise the value of alternative legal bases. A more balanced and pragmatic approach to data protection is needed, one that also takes into account what consumers and businesses would benefit from and that understands the role of all the legitimate grounds for data processing.

---

[10] E.g. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

[11] Data Protection in Contractual Relationships (Art. 6 (1) (b) GDPR), Prof. Dr. Martin Nettesheim, 2023: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4427134

III. Guarantee harmonised implementation

The GDPR created a new architecture for the protection of personal data which needs to be adequately and uniformly implemented and enforced across the board.

6. Ensure coherent implementation of the GDPR across all EU legislation

It is a fact that the GDPR has established a framework and guiding principles that act as a basis for a lot of new legislation in the Digital Single Market. One of the strengths that the GDPR brought about was to allow businesses enough time to set up processes to make it work as seamlessly as possible.

In this regard, the Commission needs to take all the necessary steps to ensure that overlaps or conflicts are avoided between the GDPR and other legislative initiatives adopted after the GDPR's entry into application.

CCIA Europe and its Members have witnessed a worrying number of more recent legislative proposals that overlap, partially conflict, or selectively confine certain provisions of the GDPR. These include, but are not limited to, the Digital Services Act, the Digital Markets Act, the Data Act, the Regulation on transparency and targeting of political advertising, and the AI Act.

Introducing new definitions or reporting requirements, or reinterpreting already established principles (e.g. data minimisation principles, data portability rights, etc), might not only lead to confusion and fragmented compliance, but could also impact innovation in the design of different products and create an increasingly complex environment for all businesses to navigate.

The risk-based approach taken by the GDPR allows the data protection framework to stay future-proof and adapt to emerging technologies, and maintaining this approach should be guaranteed. Coordination is needed by the Commission, the EDPB, and other relevant regulators to ensure appropriate guidance is provided to businesses and public authorities. Further, any new legislative proposals from the Commission must carefully consider potential areas where overlap might occur and take the necessary steps to avoid any contradiction with the GDPR.

7. Strengthen the One-Stop-Shop mechanism

Legal certainty for both businesses and users is crucial whenever implementing any new legislation. The GDPR introduced what was presumed to be a pillar for consistency and harmonisation in the enforcement of its rules: the so-called 'One-Stop-Shop mechanism'. It would guarantee a simplified process with the lead supervisory authority (LSA) in each EU Member State acting as a single interlocutor for businesses providing services in multiple EU jurisdictions.

Six years after the entry into application of these rules, we have seen multiple situations where concerned supervisory authorities (CSAs) significantly interfere in the decisions, through the cooperation and consistency mechanisms as well as through joint operations. Moreover, there are a number of examples of Member States focusing on, or favouring,

different aspects of the GDPR implementation. This has on occasion led to divergent interpretations by different supervisory authorities. Case law by the Court of Justice of the EU seems to also have reinforced this possibility.[12]

Having the LSA as a single interlocutor has been welcomed by organisations of all sizes, as it simplifies procedures and provides consistency in the implementation of the rules. Upholding the One-Stop-Shop mechanism is fundamental for a correct application of the data protection rules across the whole European Union.

CCIA Europe and its Members are also increasingly concerned about further divergences stemming from sector-specific legislation, which increases uncertainty for businesses and consumers as well as the overall efficiency of the Digital Single Market.

In this context, further guidance on the rules that govern the relationship among supervisory authorities would be welcome as it would allow not only to promote a consistent interpretation of data protection rules across the EU but also increase efficiency in investigation procedures and in overall enforcement.

8. Avoid fragmentation in Member State implementation

One of the main shortcomings in the application of the GDPR has been the continued fragmentation on implementation of the data protection provisions in different Member States.

Some examples of this fragmentation include, but are not limited to, the minimum age requirement for consent (which differs across Member States), varying territorial scopes for national data protection laws, and the different interpretation of key concepts pertaining to personal data (e.g. anonymisation, data minimisation, special categories of data, joint controllership).

CCIA Europe believes this could be addressed through additional guidance as well as through a stronger coordination role for the EDPB, who shall ensure that data protection authorities stay consistent in their interpretation, compliance, and enforcement of the GDPR. In parallel, the Commission needs to act as a guardian of the data protection framework, ensuring that data protection authorities do not interpret the GDPR in ways that lead to confusion or increase legal uncertainty.

It is of the utmost importance that the GDPR is applied equally and consistently across the EU, not only for those businesses processing data in more than one Member State, but also to avoid raising barriers for businesses thinking of entering different markets. In this respect, additional guidance by the Commission and further cooperation would help solve differing approaches and provide public authorities the needed clarity as regards a uniform interpretation of the rules.

[12] In Case C-252/21, Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social), 4 July 2023, the CJEU permits a competition authority – and potentially any authority other than data protection supervisory authorities – to examine the compliance of a company's practices with the GDPR, subject to minimal cooperation with the competent data protection authority: https://curia.europa.eu/juris/document/document.jsf;jsessionid=8462F5F83062862AD627F9EAD59D25D7?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1299124

Conclusion

The GDPR has undoubtedly created a regime that protects the privacy of EU citizens, built a stable regulatory framework that provides companies across Europe legal certainty, and has awarded consumers further protection of their personal data.

CCIA Europe considers that the GDPR has established a strong data protection framework that does not warrant to be reopened. Most of the challenges referred to above could be addressed with further guidance from the European Commission on the interpretation of certain provisions, the development of further codes of conduct, further involvement of all the interested stakeholders in the drafting of new proposals at the outset, strengthened cooperation with data protection authorities, and with increased efforts by the Commission to guarantee a harmonised implementation of the GDPR throughout the 27 EU Member States.

CCIA Europe and its Members look forward to continuing to productively engage with the Commission to ensure that the data protection framework and the overall implementation of the GDPR stay consistent and to guarantee legal certainty for businesses throughout the European Union.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009. CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.

Visit ccianet.org/hub/europe/ or x.com/CCIAeurope to learn more.

For more information, please contact:
CCIA Europe's Head of Communications, Kasper Peters: kpeters@ccianet.org