Position on the European Commission's second report on the application of the General Data Protection Regulation

PostEurop

Published by POSTEUROP
Brussels, 28 November 2024
Transparency register ID: 092682012915-24

PostEurop

ABOUT POSTEUROP

POSTEUROP is the association which represents European postal operators since 1993 and is officially recognised as a Restricted Union of the Universal Postal Union (UPU).

It is committed to supporting and developing a sustainable and competitive European postal communication market accessible to all citizens and ensuring a modern and affordable universal service.

Its Members employ **1.6 million people** and deliver billions of items annually to over **295 million homes** and **48 million companies** across Europe.

Association of European Public Postal Operators *AISBL*

Boulevard Brand Whitlock 114
1200 Brussels
Belgium

T: + 32 2 761 9650
E: info@posteurop.org

CONTEXT

PostEurop supports the ongoing consideration of the application of the GDPR as well as of the challenges arising in that regard.

PostEurop recognises the aims and benefits of the GDPR framework, to encourage the development of a coherent and reliable data protection framework, for the benefit of citizens as well as society more broadly.

However, it is critical that this framework is clear, foreseeable and operationally workable. The GDPR must provide "legal and practical certainty for economic operators and public authorities".

Compliance with the GDPR within the broader, rapidly evolving EU regulatory framework, both from a technological and economic perspective, is at risk of becoming extremely challenging if universal postal service providers are to continue to provide sustainable and thriving postal services, as well as ensure the economic contribution that such postal services and service providers make.

Our submission focuses on those parts of the Report that are most relevant to the data protection aspects affecting our postal business and other related services to postal users.

In particular, PostEurop seeks that the application of the GDPR in practice takes into account the postal services sector's specific features, which emanate from the social, cultural and economic objectives inherent in the provision of services to meet postal users' needs. It also advocates for a high level of coherence in relation to the broader EU digital and data legislative framework to ensure that innovation and evolution of the postal service is not compromised.

PostEurop supports the following conclusions and recommendations in the Report[1]:

That the EDPB and DPAs are invited to:

- Engage in constructive dialogue with controllers and processors on compliance with the GDPR.
- Explore ways/tools to further assist data exporters in their compliance efforts in relation to the Schrems II requirements.
- Establish regular cooperation with other sectoral regulators on issues with an impact on data protection, in particular those established under the new EU digital legislation, and actively participate in EU-level structures designed to facilitate cross-regulatory cooperation.
- Make fuller use of the tools for cooperation provided by the GDPR, so that dispute resolution is used only as a last resort.
- Implement more efficient and targeted working arrangements for guidelines, opinions and decisions and prioritise key issues in order to reduce the burden on data protection authorities and to respond more quickly to market developments.

That the Commission will:

- Build synergies and consistency between the GDPR and all legislation touching upon the processing of personal data based on experience and, if necessary, take appropriate actions to provide legal certainty.
- Reflect on how to better address the need for structured and efficient cross-regulatory cooperation to guarantee the effective, consistent and coherent application of EU digital rules, while respecting the competence of data protection authorities for all questions concerning the processing of personal data.
- Use all available means to deliver expedient clarifications on matters of importance to stakeholders, in particular by requesting opinions of the Board.
- Cooperate with international partners on facilitating data flows – including if made on the basis of model contractual clauses.
- Support ongoing reform processes in third countries on new or modernised data protection rules by sharing experience and best practices.
- Engage with international and regional organisations such as the OECD and G7 to promote trusted data flows based on high data protection standards, including in the context of the Data Flow with Trust initiative.

[1] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Second Report on the application of the General Data Protection Regulation COM/2024/357 final (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52024DC0357)

POSTEUROP GENERAL COMMENTS ON THE GDPR

Balancing fundamental rights and key principles

The GDPR makes clear that the fundamental rights to privacy and data protection must be balanced against other fundamental rights. This includes the right to carry on legitimate business activities as well as the rights of EU citizens to avail themselves of services of general economic interest.

These overarching principles must be recognised in enforcement approaches. Reliance on data subject consent should not become the default position. This would ignore the balancing of rights clearly envisaged by the GDPR, as well as the accountability of the controller and other lawful bases explicitly provided for.

PostEurop recognises the importance of the Charter of Fundamental Rights and the European Convention of Human Rights in this domain. These too protect a wide range of rights and interests, all of which must be effectively balanced.

Complexity and cost

Complexity and cost present significant challenges to business compliance with the GDPR framework, even for large entities.

Businesses face difficulties in managing the interplay between the GDPR and other legislative or regulatory instruments affecting use of personal data, including the regulation of consumer rights, digital services, specific technologies, cybersecurity and the use of non-personal data.

The significance of postal services to consumers and businesses remains, while innovations are simultaneously required to meet evolving user needs. Uncertainty remains in relation to key definitions as well as overlapping frameworks and potential enforcement approaches. This leads to a complex regulatory landscape. It is also contrary to the basic legal and regulatory principle that businesses should be able to plan their activities with clear knowledge of the legal consequences.

Guidelines which are theoretical or only reiterate the law do not suffice; guidance as to the practical solutions which are acceptable are required and in a timely manner.

Risk based Approach

The principle of accountability and the risk-based approach reflect a flexible application of data protection principles while recognising the responsibility of controllers. Recitals 74 and 76 of the GDPR make clear that data controllers should assess the likelihood and severity of risk to the rights and freedoms of data subjects.

The challenge of pursuing a risk-based approach in GDPR compliance is the obligation not (only) to have regard to the risks for the controller / economic operator, but to also have due regard to the rights and freedoms of data subjects.

Operationalising this in practice is extremely difficult.

While guidance makes clear that a DPIA must be a genuine assessment of risks, it also allows controllers to take measures to address them. However, there is little guidance on how to actually assess necessity and proportionality, nor on the practical tools required to manage any identified risks to the rights and freedoms of data subjects resulting from the processing of personal data.

At the same time, further guidance and clarity on specific aspects of data subject rights are required, such as the protection of the rights of minors. In its report, the Commission states that children require specific protection when their personal data are processed and that there is increasing focus on the need for effective and privacy-friendly age verification tools. It is important that the work launched by the European Commission at the beginning of 2024 on the subject progresses quickly.

A clear need for consistency

There is a real need for consistency, particularly with regard to the decisions of the supervisory authorities, which often lead to a restrictive interpretation of the GDPR, and also with regard to the relationship between the GDPR and the new obligations arising from the European digital strategy.

The GDPR marks the desire for harmonisation at a European level. It aims to strengthen the rights of European citizens, but also to make companies and organisations that process personal data more accountable. However, it refers back to national frameworks, which inevitably risks leading to differences in application between Member State DPAs. PostEurop notes that these variations have been recognised in the Report and that it has led to a greater level of inconsistency and fragmentation than specific national legislative measures.

An often-restrictive interpretation of the GDPR

An opportunity to have constructive consultations with DPAs would enhance compliance, and also more meaningful public consultations by the EDPB.

Guidelines sometimes excessively restrict the room for manoeuvre left by the GDPR, including in matters related to the e-Privacy regime. As a result, many companies apply a precautionary principle and are reluctant to embark on projects that seem too complex or too costly to implement in view of the many constraints associated with the GDPR.

The Report has clearly identified concerns in this regard and PostEurop supports the following:

- That supervisory authorities should engage in constructive dialogue with data controllers and processors on compliance with the GDPR; and that guidelines at member state level reflect guidance or opinions issued at EU level, as well as the case law of the Court of Justice;
- That consultations on guidelines and opinions are aimed at understanding the operational and economic realities, as well as the practical implications, for businesses affected;
- That shorter, pragmatic and accessible guidelines providing clear and unambiguous guidance on the application of the GDPR are available; and are also updated to reflect experience, technological developments or legal developments.

Up to date guidance is currently lacking on certain critical issues –e.g., the concept of "personal data", which is evolving in light of recent CJEU case law and risks being unclear.

There is also an emerging risk of conflict between the concepts of "Open Data" in the EU's data policy and personal data objectives. Given the increased regulation of non-personal data, a clearer and more predictable definition of what constitutes personal data is essential.

In addition, what constitutes a "transfer" may not even be certain[2].

Guidance on practical, technical and workable solutions for economic operators is essential for compliance.

New legal challenges for data security

As the cornerstone of European regulation on the protection of personal data, the GDPR has now been integrated with new obligations arising from Europe's digital strategy, such as the Digital Markets Act, the Data Governance Act and the Artificial Intelligence Act.

In the future, however, it will be necessary to ensure coherence in the regulation of the European digital space. PostEurop notes that this has been clearly recognised in the Report.

The intertwining of issues and challenges can sometimes lead to contradictions or blockages that necessarily undermine the desired objectives. The new uses of data and the acceleration of digitisation within organisations and businesses encourage the processing of increasing quantities of data, thereby increasing the risk to privacy and data security.

Recurring difficulties encountered when transferring data outside the European Economic Area (EEA)

Transferring personal data outside the European Economic Area (EEA) has become a major challenge for most organisations. The annulment of past adequacy decisions, as well as on-going challenges, has resulted in considerable legal uncertainty as to what solutions and mechanisms will be acceptable to national DPAs, the EDPB and the courts.

The key concept that the risk-based approach applies to the entirety of obligations of controllers and processors, including Chapter V GDPR (International Transfers), should be clearly recognised.

PostEurop notes that the need to take into account the specific nature of the transfer, as well as the challenges still arising in international transfers, have been clearly recognised in the Report. PostEurop agrees that recognition of unique needs and features in the application of Chapter V GDPR on international data transfers is required[3].

Inconsistencies in approach should also be resolved. For example, the application of a risk-based approach having due regard to the rights and freedoms of data subjects is evident in guidelines

[2] A recent decision of the EDPS concerning the use of video conferencing software by the CJEU (based on Regulation (EU) 2018/172519) found that since the data importer was contractually excluded from having access to the personal data processed by the data exporter and such data were encrypted, there was no data transfer within the meaning of EU data protection law. EDPS Decision on the Court of Justice of the EU's request to authorise the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. for transfers of personal data in the Court's use of Cisco Webex and related services, 13 July 2023, case 2023-0367

[3] Report, pages 19-20.

issued on DPIAs (although lacking specific guidance[4]) and yet the approach remains unclear and uncertain in the guidelines on international data transfers.

The obligation to consider additional protection measures (when relying on SCCs) is extremely challenging in practice. The burden on economic operators to assess domestic legislation in non-EEA countries is disproportionate. Failures to provide clear and workable guidance in the area fails to recognise the realities, and needs, of globally interconnected service providers.

It is difficult to choose between the different measures proposed by the EDPB. Indeed, if access to personal data by public authorities is permitted in the importing country, technical measures (in particular encryption) need to be considered. However, guidance is required to support the operationalisation of privacy concerns and reflecting the practical economic realities of a situation. The Report recognises that the specific features of each transfer may differ[5], but it is unclear how the cursor should be placed between the different categories of data transferred.

A more pragmatic and innovative approach may be required more generally in relation to international data transfers.

PostEurop welcomes support for efforts at an intergovernmental level.[6] Matters such as regulation of government access are not easily dealt with at economic operator level.

PostEurop further notes that the need for practical guidance on transfer impact assessments, as well as a more harmonised approach, has been taken into account in the Report.[7]

Lastly, solutions are required to reconcile the defence of European values, such as the protection of citizens and their data, with the digital development of European businesses:

- Policymakers and EU data protection authorities should provide additional guidance on the issue of unlawful transfers. Different analyses do not promote legally secure data transfers.
- The introduction of third-party monitoring mechanisms, including internationally recognised standards, could make it possible to check that the importer is complying with the contractual conditions of the transfer and the security measures.
- The supervisory authorities should also be clearer and state their position on the issue of transfers.

Improvements needed to enable players to be identified

Institutional measures must be refocused to ensure that affected economic operators can act within clear, practical and predictable parameters and that the key practical concerns are addressed.

The legal classification of the various players can still give rise to considerable legal uncertainty.

The case law on joint controllers is evolving, but the position on responsibility of each party remains vague in practical terms.

It would be appropriate to more clearly define how the responsibilities of separate controllers should be differentiated and delineated where joint controllership arises. PostEurop notes that the Report has recognised the need for clarification of the various roles.

Finally, the position of economic players providing the technical solutions should be considered more closely.

Such providers should not inevitably default to the position of a processor within the meaning of the GDPR, even when it has clearly determined all the purposes and means of the processing linked to its service. The suppliers of these services do not wish to be described as data controllers. It would be appropriate to provide concrete answers to this question.

PostEurop appreciates the opportunity to submit comments on the Commission's Report.

---

[4] The guidance on DPIA7 7 WP29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248 rev. 01, 4 October 2017, does not address key points such as the exact methods for risk assessment (Article 35(7)(c) GDPR), or for proportionality and necessity assessment (Article 35(7)(b) GDPR)).

[5] Report, pages 19-20, para. 7.1.

[6] Report, pages 25-27.

[7] Report, pages 22-23.

For more information,

please contact:

Ms Christelle Defaye-Geneste

Chair of PostEurop European Union Affairs Committee
La Poste Groupe

E: christelle.geneste@laposte.fr
T: +33 155 440 181

Ms Sarah Gallagher

Chair of PostEurop Data Protection Working Group

E: sarah.gallagher@anpost.ie
T: +353 1 705 8432

POSTEUROP contact:

Association of European Public Postal Operators *AISBL*

Boulevard Brand Whitlock 114
1200 Brussels
Belgium

E: info@posteurop.org

T: + 32 2 761 9650

Photo credits: istock