Position Paper

FERMA Feedback to the European Commission's Roadmap Document:

"Report on the application of the General Data Protection Regulation"

28 April 2020

I. Introduction

The Federation of European Risk Management Associations (FERMA) thanks the European Commission for this opportunity to share it thoughts on the implementation of the GDPR and feedback on the Roadmap document "Report on the application of the General Data Protection Regulation".1 FERMA also attaches in annex its 2019 report "GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation".2

Based on its membership of 5000 European risk managers across the European Union, many of whom are Data Protection Officers (DPO), FERMA is uniquely placed to offer valuable feedback on the implementation of the GDPR. FERMA trusts the Commission will consult the results of FERMA's report with interest and factor these into its own report moving forward.

II. Assessment of the Evaluation Report's scope

FERMA thinks the existing scope of the evaluation scope is relevant. Covering issues of international transfer of personal data to third countries, and the cooperation and consistency mechanism between national data protection authorities, FERMA believes the scope should provide legal certainty especially for how national data protection boards will enforce GDPR compliance, and especially on the interpretation of what constitutes "high" risks. According to FERMA's GDPR and Corporate Governance report, 30% of respondents list uncertainty and complexity as the number one challenge for GDPR implementation.

In particular, the cooperation and consistency mechanism is critical to improve the harmonisation of data protection enforcement and compliance across the European Union. To further support harmonisation, FERMA encourages the Commission to work with the European Data Protection Board (EDPB) to continue issuing useful guidance and coordinating among the data protection authorities of

[1] Roadmap, Ares(2020)1873825. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation

[2] GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation, (November 2019). Available at: https://www.ferma.eu/advocacy/gdpr-corporate-governance-the-role-of-internal-audit-and-risk-management-one-year-after-implementation/

the Member States.3 Furthermore, the European Commission should consider supporting cooperation between industry bodies and national data authorities as it clarifies the technical and financial aspects of the GDPR.

III Areas to Improve the Scope of the Evaluation Report

While the Evaluation Report addresses important topics, FERMA agrees with the Council that the scope of the evaluation should be broadened to have a more comprehensive evaluation of the GDPR.4 With that in mind, FERMA identifies two main areas where the Commission's Evaluation Report scope could be broadened to further improve the implementation of the GDPR.

a) Corporate Culture Shift Towards Data Protection

Since entry into force, the GDPR has generally led to a positive shift in the corporate culture in regards to the data protection. This is having further positive flow on effects in other areas such as the need for robust cybersecurity. FERMA results show, for example, that 91% of risk managers have implemented measures to prevent and deal with data security breaches. These measures include embedding privacy risk assessments in new services and products, and setting up business continuity/crisis management plans.

FERMA also points to the positive role which risk managers have with regards to implementation of new technologies so that a risk assessment is conducted prior to implementation. Preliminary findings of FERMA's European Risk Manager Survey 2020 show that 37% of respondents identify and assessment risks prior to adoption of new technologies.5 To help manage those risks, risk managers maintain a stable and high level of collaboration with IT (43% of them have close collaboration and 6% the activity within their team) and information security teams (45% of them have close collaboration and 10% the activity within their team).

However, although good progress has been made, further efforts should be directed towards fostering a corporate cultural of data protection and promoting corporate governance since it plays a key role in GDPR compliance.6 FERMA is convinced a culture shift can be brought about using corporate risk management methodologies such as Enterprise Risk Management (ERM) and the Three Lines of Defence model that in turn builds accountability within organisations.

In this regard, FERMA understates the critical role of data protection officers (DPO). FERMA's findings show that the DPO is usually assigned to an existing function within organisations, such as legal/compliance (54%), IT/IS (15%), Risk Management (11%) or Finance/Operations (10%). More importantly, most organisations establish strong links between the DPO, risk management, and internal audit functions. For better implementation and compliance of the GDPR moving forward, FERMA strongly recommends that European institutions consider further promotion and support of

[3] Council position 14994/1/19 (19 December 2019) "Council position and findings on the application of the General Data Protection Regulation (GDPR)." See sec. §7.
[4] *Ibid*., §6
[5] *FERMA European Risk Manager Survey 2020,* (Forthcoming)
[6] European Data Protection Board. "Contribution of the EDPB to the evaluation of the GDPR under Article 97", (18 February 2020), p. 3: touching upon the topic of a common culture of data protection. Available at: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

corporate governance structures that do not isolate the DPO, but instead, integrates strong cooperation between the risk specialist and the DPO. The Commission should recognise the relationship of privacy risks between the DPO, risk management and internal audit relying on the 'Three Lines of Defence' model as a starting point. Doing so will encourage organisations to move beyond mere compliance towards a culture of robust data protection.

b) Aligning GDPR with Innovation

Another area for examination not covered in the Commission's scope is the effect the GDPR has on innovation. In this regard, FERMA shares many of the concerns highlighted by the Multistakeholder Expert Group.7 In particular, based on feedback from FERMA members, the GDPR is the second greatest challenge for companies (25%) in the area of innovation due to a lack of legal certainty when incorporating innovation in business processes while addressing data privacy concerns. FERMA highlights once again the need for the DPO to be integrated to the greatest possible extent within new business processes dealing with privacy matters, in a cross-cutting collaboration between various functions and supported by an enterprise-wide risk management framework.

IV. Conclusion

FERMA thanks the Commission for the opportunity to share its thoughts on the implementation of the GDPR. The Commission should consult the results of FERMA's own report on the GDPR and factor those results into the final evaluation report. Furthermore, FERMA encourages the Commission to consider a wider scope of the report and recommends including:

- The role played by corporate governance, and the use of corporate risk management methodologies such as Enterprise Risk Management and the 'Three Lines of Defence' model to shift corporate culture towards data protection
- Assessing the effects GDPR is having on innovation and to propose mechanisms that could further support innovation.

FERMA remains committed to working with the Commission and offering the insights of its membership to improve the implementation of the GDPR.

[7] Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679. "Contribution from the Multistakeholder Expert group to the stock-taking exercise of june 2019 on one year of GDPR application" (13 June 2019), p. 15. Available at: https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf