FIVE YEARS OF GDPR IN THE DATA AND MARKETING INDUSTRY

INTRODUCTION

Five years after its adoption, the impact of the General Data Protection Regulation (GDPR) on Europe's data protection and privacy landscape cannot be overstated. Not only did the GDPR provide upgraded rights to individuals and aimed at harmonising the rules across the continent; its effect went beyond Europe to influence the debate around other countries' data protection legislation and spark renewed interest in issues of data privacy.

However, despite the attempts of EU Member States, the European Commission, and the European Data Protection Board (EDPB) to ensure a consistent application of the law, fragmentation remains, ultimately contradicting the harmonisation goal of the GDPR.

FEDMA's position paper reflects the five-year experience of the Data and Marketing Industry with the GDPR, identifying the following key areas of improvement:

I. **GDPR Risk-based approach**: Setting the risk-based approach as the decision-making compass in the interpretation and implementation of the GDPR

II. **GDPR oversight by Data Protection Authorities (DPAs)**: Promoting an inter-regulatory approach in the implementation and enforcement of the GDPR

III. **GDPR legal bases for data-driven marketing**: Promoting the added value of Legitimate Interest for data subjects

IV. **International Data Transfers**: Enhancing proportionality and legal certainty

V. **Privacy Enhancing Technologies (PETs)**: Encouraging organisations to invest in pseudonymisation and anonymization techniques

VI. **Data controller & data processors**: Preserving a clear and proportionate allocation of responsibilities

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

I. GDPR RISK-BASED APPROACH: Setting the risk-based approach as the decision-making compass in the interpretation and implementation of the GDPR

Five years after the entry into force of the GDPR, companies in the Data and Marketing Industry view the EU data protection framework as a guarantee of trust for their customers. By providing precise information on the processing of personal data and the rights available to customers, companies significantly improve their image and reputation. In this context, as individuals are increasingly aware of their rights under the GDPR and make full use of them, **marketers consider their obligation and ability to promptly respond to data subjects' requests as a relevant proof to ensure a trustworthy relationship with their customers.**

Compliance with the GDPR is therefore seen as a potential competitive advantage even *vis-à-vis* non-EEA-based organisations. As such, over the past five years, marketers made significant investments to ensure compliance with the GDPR, especially in data collection and management systems, data governance, IT infrastructures, human resources (DPOs, legal experts, privacy engineers), tools and processes to handle data subjects' requests and Privacy Enhancing Technologies (PETs),

In practice, however, companies in the Data and Marketing Industry still face significant hurdles in order to comply with the GDPR, often outweighing the benefits of a trustworthy relationship with their customers. Marketers consider the strict and divergent interpretation of the GDPR by national Data Protection Authorities (DPAs) as the main impediment and source of legal uncertainty, preventing them from reaping the benefits of the data economy while ensuring the protection of their customers' personal data.

Specifically, marketers underline the **failure by DPAs in applying the risk-based approach of the GDPR to the modern data economy**. Reflected in a number of provisions (e.g. Art 24 on accountability, Art. 25 on the principles of privacy by design and privacy by default, Articles. 33 and 34 on governing the management of a data breach, Article 32 on security, etc.) the GDPR's risk-based approach means that data controllers are encouraged to implement protective measures corresponding to the level of risk of their data processing activities, taking into account the likelihood and severity of the risk on the rights and freedom of individuals. However, in practice, the GDPR is generally interpreted in a conservative and one size-fits-all manner by a number of Data Protection Authorities (DPAs), even when the risk of the processing is purely theorical and trivial, thus creating many tensions and disruptions. In the Data and Marketing Industry, for example, **the level of risk associated to the processing of personal data for marketing purpose is low as marketers do not need a 360-degree view of their customers nor processing highly sensitive data, to support marketing operations, product innovation and customer experience.** Yet, the view of some DPAs that even pseudonymised

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

marketing data can entail significant risks for the data subjects[1] whereas in another case a supervisory authority refused to exercise its corrective powers where a controller had used pseudonymization as measure to mitigate risks for individuals[2], further underline a lack of common culture among DPAs.

As such, **there is a general perception in the Data and Marketing Industry that regulators are favouring the sole objective of personal data protection over other public policy objectives**, including the protection of other fundamental rights as per Recital 4 GDPR such as the Freedom to conduct a business (Art.16 CFR). They are doing so regardless of the actual level of risk for the rights and freedoms of individuals the data processing activities at stake, whereas the GDPR provides that they have to be "determined by reference to the nature, scope, context and purposes of the processing"[3]. In this context, despite huge investments in GDPR compliance, most organisations in the Data and Marketing Industry have experienced a negative impact on innovation, customer prospection and a competitive disadvantage *vis-à-vis* bigger players. If not properly addressed, the lack of a risk-based approach will have an adverse impact on smaller players, especially SMEs, which rather refrain from taking on innovative project than risking a fine with no possibility to appeal in court due to their limited resources. The need for a risk-based approach is even more important in the context of nascent technologies such as AI whose need to process personal data for algorithmic training will need to be assessed pragmatically to enable the development of new innovative products and services.

More generally, there is a growing concern that by ignoring the risk-based approach and the principle of proportionality based on the reconciliation of competing objectives, the current approach is not up to the European Data Strategy set out by the European Commission which risks falling short in fostering innovation and enabling emerging companies to process the necessary data for the effective training of algorithmic models for the development of new products and services able to compete at the international level.

FEDMA's Recommendations:

EU policymakers and DPAs should:

- Apply in a consistent manner the GDPR risk-based approach stemming from GDPR and the general principle of proportionality

[1] Mind Media, 21 March 2023, Amende de 60 millions d'euros par la Cnil : Criteo dénonce une position "anti-publicité en ligne" – YOU COULD ALSO REFER TO THE FRENCH EDF CASE
[2] General Court of the European Union, SRB v EDPS, 26 April 2023, Case T-557/20, , para. 32.
[3] See Recitals 75 and 76 of the GDPR

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

- Reconciliate the fundamental right of data protection with other fundamental rights and public policy objectives.

II. DATA PROTECTION AUTHORITIES: Promoting an inter-regulatory approach in the implementation and enforcement of the GDPR

Most organisations in the Data and Marketing Industry highlight a difficult relationship with DPAs. This is mostly related to the abovementioned argument that **DPAs lack a balanced approach between data protection and use for business with a sometimes-broad and too-legalistic interpretation of the GDPR.** This is, for instance, reflected in :

- the CNIL's fine to utility company EDF where the French DPA reprehended, amongst others, the failure to provide data subjects with an exhaustive and updated list, including the exact identity, of partner recipients whereas the provisions of the GDPR (art. 13 and 14) as well as the Court of Justice of the EU (CJEU)[4] state that there is no need to inform the data subject of the identity of all successive data controllers when collecting consent, but only "recipients or categories of recipients".
- the interpretation by the Dutch DPA that the Legitimate Interest legal basis[5] cannot be relied upon for commercial interests,
- the CNIL's position that when relying on consent through contractual commitments of partners, the controller is under the obligation to audit such partners, including in controller to controller or joint controller relationships.[6]

This excessively conservative approach to data protection is also accompanied by **a misuse of the full range of GDPR's corrective measures** whereby the imposition of fines has become the *de facto* enforcement model. Other GDPR corrective options, including warning, reprimand, order to bring processing operations in compliance, etc., might instead be much more efficient, proportionate and dissuasive in light of the specific circumstances of the case. Fines should thus remain a last-resort option for the most serious, repetitive cases or those that create real harm for individuals.

According to organisations in the Data and Marketing Industry, the use of fines as a one-size-fits-all solution also exposes the **lack of a more sectoral approach by DPAs**. Though DPAs are responsible for the oversight of data protection legislation in every domain and sector, there is a lack of expertise

[4] Court of Justice of the European Union, 27 October 2022, Case C-129/21
[5] European Commission, 6 March 2020, Letter of the European Commission to the Dutch DPA regarding the interpretation of the Legitimate Interest legal basis
[6] Mind Media, 21 March 2023, Amende de 60 millions d'euros par la Cnil : Criteo dénonce une position "anti-publicité en ligne" – YOU COULD ALSO REFER TO THE FRENCH EDF CASE

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

and understanding of the specific business models that they regulate. This is, for example, seen in the guidelines issued by DPAs which, despite being helpful GDPR-compliant tools, they lack the necessary pragmatism, thus leading to legal uncertainty and unnecessarily costly processes for the practical implementation and compliance of certain rules in specific domains and sectors. Hence, in the absence of more sectoral experts within the DPAs' staff, **national authorities should focus more on cooperation with other sectoral competent authorities.** In the Netherlands, for example, the regulators for media, data protection, financial markets, consumer protection and competition have set up a Digital Regulation Cooperation Platform to work together in regulating the digital services which they respectively oversee.

In parallel, **DPAs should also support stakeholders' engagement and co-regulatory approaches for specific sectors and domains**, especially via Codes of Conduct (CoC) and certifications which, once approved, could also unburden part of the workload of Data Protection Authorities (DPAs). For instance, the Spanish DPA recently revised a CoC on the processing of personal data for advertising activities[7] which provides for, among others, an online out-of-court dispute settlement mechanism for resolving data protection disputes between adhering entities and data subjects. In other words, rather than on sanction-based enforcement, **DPAs should favor constructive solutions that reconcile protection of personal data with the activity of the actors concerned in a given sector and a reasonable balance of benefits and risks related to the use of data in line with the principle of proportionality.**

Finally, though companies in the Data and Marketing Industry welcome the possibility to provide comments before the final adoption of the EDPB or DPA guidelines, an early involvement in the process would be desirable. Consulting stakeholders at a sufficiently early stage before the first version of the draft guidelines would incentivize DPOs and other experts to invest time in the process and it would support a trustworthy relationship with the regulators while avoiding a top-down approach. Currently, there is a general perception that the feedback provided following the publication of draft guidelines has limited chances to introduce new concepts and ideas, thus disincentivizing stakeholders from responding to a consultation. Such constructive engagement would also help DPAs better understand the business models they are regulating.

FEDMA's Recommendations:

EU policymakers and DPAs should:

[7] AUTOCONTROL, CODE OF CONDUCT DATA PROCESSING IN ADVERTISING ACTIVITIES

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

- Promote a more sectoral approach supported by co- and self-regulatory initiatives in favor of a more tailored and balanced implementation of the GDPR.
- Provide shorter guidelines with more concrete examples to facilitate their uptake by companies.
- Apply the full range of corrective measures under the GDPR to ensure that enforcement is efficient, proportionate and dissuasive in light of the specific circumstances of a case.
- Set up a pre-consultation phase before issuing draft guidance, to gather input from relevant stakeholders.

III. GDPR LEGAL BASES FOR DATA-DRIVEN MARKETING: Promoting the added value of Legitimate Interest for data subjects

The GDPR provides organisations with a range of legal bases for processing and organisations can choose a basis that is appropriate to their particular processing activity. All legal bases for processing are on equal footing with one another, meaning that there is no "default" legal basis, no hierarchy between them, and none should be privileged over the other. However, **marketers point out a significant degree of uncertainty and misconceptions about the legal basis for processing personal data for marketing purposes, often resulting in an over-reliance on consent.**

Such over-reliance on consent in the data and marketing industry stems from an interpretation by some DPAs and a narrative which privileges consent over legitimate interest, portraying the former as a processing ground that gives individuals more control and provides for more legal certainty even where consent is less suitable to the processing at hand and results in lower privacy outcomes when compared to Legitimate Interest.

FEDMA believes that this approach disregards the fact that **individuals increasingly express "consent fatigue" as they are constantly asked to make meaningful decisions at speed, multiple times during the day on the basis of information often related to complex processing scenarios**. In other words, the consent ground puts all the responsibility and onus on the data subjects who are expected to endlessly conduct a balancing test themselves. In parallel, though the current narrative unfairly portrays Legitimate Interest as the lesser ground with a potential adverse impact on data subjects, it overlooks the benefits of Legitimate Interest. In contrast to consent, Legitimate Interest shifts the responsibility on data controllers to make the balancing test while still providing data subjects with the necessary information and the indisputable right to opt-out as all GDPR provisions continue to bind the data controller. In other words, **relying on the legitimate interest legal basis is not a blank check given to the controller as, in addition to complying with the GDPR, it has to perform a formal**

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

legitimate interest assessment (LIA) balancing its own legitimate interest versus individual interest and identifying possible mitigation measures.

As such, while Recital 47 of the GDPR recognizes that Legitimate Interest may be relied upon for marketing purposes, companies shield away from using legitimate interest where appropriate because too risky and complex. Despite five years since the entry into force of the GDPR, uncertainty over the use of Legitimate Interest has already caused organisations in the data and marketing industry to cancel activities and projects, negatively affecting revenue opportunities and innovation.

This is for example reflected in the ongoing debate on direct mail in Germany where there is a lack of consensus among DPAs on the appropriate legal basis for address data trading. Currently based on Legitimate Interest which gives the specific right of the recipients concerned to object to such data processing under Article 21 (2) GDPR, address data trading enables companies to reach out to new potential customers. However, as some DPAs in Germany (e.g. Baden-Württemberg, Berlin) hold that such processing can only take place with the prior consent of the respective recipients, some companies refrain from taking the risk of being sanctioned, thus curbing new customer promotion. On the opposite side of the spectrum, the Austrian DPA approved a Code of Conduct under Art.40 GDPR for the Austrian direct marketing industry allowing the transmission and use of list data based on legitimate interest.

As such, faced with legal uncertainty which carries the risk of being fined, companies often take the safest option, with unintended negative consequences for innovation. However, **even where marketers rely on consent as the default option because of uncertainty over the legitimate interest legal basis, they still face significant issues and implementation costs in complying with the requirements for consent**. Some of these challenges include:

- Setting up systems for tracing and time-stamping consent in order to provide proof that consent was lawfully collected;
- Providing, as data processors, comprehensive lists of data controllers to obtain informed consent, where the data processors rely on data providers on behalf of the controllers;
- Obtaining consent by telephone because of the need to record customer identification which customers perceive as intrusive;
- Assessing to what extent a consent request must be specific such as whether separate marketing campaigns addressed to the same data subject require separate consent

Finally, **organisations are also disincentivized in using Legitimate Interest as a legal basis for marketing purposes due to the need of carrying out legitimate interest balancing assessments (LIA) which are not tailored to their processing activities or sector**, often resulting in time-consuming procedures. As such, a constructive dialogue between DPAs and interested stakeholders should incentivize the

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

adoption of Codes of Conduct and certifications to provide templates LIA for different types of activities enabling organisations to easily assess whether they have a legitimate interest, the evidence they need to provide, and the parameters for not extending that legitimate interest further than is intended.

FEDMA's Recommendations:

EU policymakers and DPAs should:

- Promote a more balanced narrative that does not set consent as the default legal basis with the highest level of effective data protection.
- Incentivise and clarify marketers' reliance on legitimate interest subject to full compliance with the GDPR.
- Enable a constructive dialogue with relevant stakeholders for developing templates for legitimate interest balancing assessments (LIA) for different types of activities via Codes of Conduct and certifications.

IV. INTERNATIONAL DATA TRANSFERS: Enhancing proportionality and legal certainty

Following the invalidation of the EU-US Privacy Shield in the Schrems II Case by the CJEU, transferring personal data outside the EEA has become a significant challenge for most organisations in the Data and Marketing Industry, except where the data was already localized in the EU.

Alternative equivalent solutions to U.S. large companies' transfer tools are often difficult to find as similar European services are still developing and may be less mature and efficient. As a result, many organizations have turned to implementing the supplementary measures outlined in the EDPB's guidelines and as per the CJEU's decision. However, companies setting up the new protective measures, especially to avoid the potential risk of non-EEA public authorities' access to data, have incurred in significant costs stemming from:

- De-commissioning non-compliant transfer tools and replacing them with new solutions which often provide less service performance.
- Carrying out the required impact assessment of third countries' legislation or hiring external consultants to do it.
- Setting up technical encryption measures which are nevertheless problematic as often the keys remain under the exclusive control of the data controller.
- Bringing subcontracts with partner organisations into conformity when local legislation provides for potential unlimited access to data by public authorities.

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

As some of these solutions can go up to an additional €300k on top of the regular license fee paid to external service providers, most marketing service providers cannot afford these costs and are thus forced to rely on lower quality EU-based service providers or downsize part of their international operations.

Though Standard Contractual Clauses (SCCs) are still considered a useful tool to facilitate compliant data transfers, **organisations in the Data and Marketing Industry struggle to operationalize SCCs due to their complicated structure**. Furthermore, following Schrems II, SCCs are often insufficient to ensure the equivalent level of protection required by the CJEU and additional protective measures are needed. However, marketers find difficult to assess the type and extent of these technical measures, especially encryption, thus often requiring external guidance. For example, it is unclear whether and what technical measures are necessary to transfer IP addresses. Finally, the difficulty of implementing SCCs arises in the context of subsequent data transfers as data exporters find problematic to ensure the compliance of the transfer framework throughout the chain, especially when the data processor relies on subsequent subcontractors who also use their own subcontractors.

FEDMA's Recommendations:

EU policymakers and DPAs should:

- Provide additional guidance regarding the issue of unlawful transfers in case of notification by the data exporter on whether the transfer instrument and complementary measures are insufficient to carry out the transfer.
- Develop an official SCC-generator at national or EU level which guides organisations via Q/A across the structure of different SCCs. Alternatively, facilitating the use of SCCs by means of an interactive dashboard.
- Provide additional tools at EU level to help companies assessing the data protection framework of third countries.

V. PRIVACY ENHANCING TECHNOLOGIES (PETs): Encouraging organisations to invest in pseudonymisation and anonymization techniques

Since the entry into force of the GDPR, Privacy Enhancing Technologies (PETs) is another area which is increasingly being explored in the data and marketing industry. Provided as an example of an appropriate data protection safeguard by the GDPR, pseudonymization is, for instance, a foundational PET technique to mitigate privacy risks by replacing private identifiers with fake identifiers or pseudonyms to hide key identifiable information. In the data and marketing industry, **pseudonymisation thus enables organisations to single out individual behaviour without directly**

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

identifying the individuals. However, though this technique has become a helpful tool for marketers to protect their data and optimise their marketing campaigns as well as a proof of trust with their customers, there remain both operational and legal challenges.

Specifically, the requirements of the GDPR, regardless of the type of processing of pseudonymised data, along with the lack of common pseudonymisation criteria for specific types and risks of category of personal data as well as the correspondent types of pseudonyms to use represents a barrier for smaller organisations to adopt this technical solution. Additionally, the lack of officially recognized/approved pseudonymisation criteria has also raised challenges from a compliance perspective whereby **certain DPAs do not recognize some pseudonymised data processing as such and look at the data processed by these companies as purely personal data of an identified individual.** As a result of these challenges, marketers have less incentives to invest resources in processing pseudonymised data, leading to a significant drawback in the relationship with their customers. In this context, FEDMA supports initiatives such as the draft GDPR Code of Conduct[8] on Pseudonymisation which would establish an EU-wide management system for pseudonymisation with general pseudonymisation requirements recognized by DPAs across the EU. In addition, pseudonymisation of data should also be considered as mitigating factor in enforcement actions.

In parallel, **marketers also stress the need for processing anonymous data under a risk-based approach, more focused on transparency and accountability rather than zero-risk unlinkability**. In the Data and Marketing Industry, anonymous data is used to identify trends within a group of targets - even without having specific information on the individual level – to tailor a specific campaign which is still relevant to the consumer. However, there is a lack of consensus on what constitutes anonymous data with the Working Party 29's Opinion on Anonymisation Techniques as well as from some DPAs holding that the only remaining solution to obtain GDPR-compliant anonymizations is to effectively delete the original dataset. As the concept of 'personal data' is bound to expand even further and, as a result, to apply to an exponentially growing range of situations, this zero-risk approach seems unfeasible for most data controllers and would in many cases contravene other legal provisions. Though court cases such as Breyer[9] seem to point to a more risk-based approach, it remains unclear to marketers how to operationalise the requirement that the risk of re-identification must be insignificant. **The more recent judgement by the General Court of the EU in SRB v EDPS[10] could already provide more legal certainty, holding that pseudonymized data transmitted to a data recipient will not be considered personal data if the data recipient does not have any additional information enabling it to re-identify the data subjects and has no legal means available to access such information**. Though a case-by-case assessment will always be necessary, this judgement may

[8] SCOPE Europe presents on "Advancing Pseudonymisation with a Universal Code of Conduct" at Bitkom's Privacy Conference 2021
[9] Court of Justice of the European Union, Patrick Breyer v Bundesrepublik Deutschland, 19 October 2016, Case C-582/14
[10] General Court of the European Union, SRB v EDPS, 26 April 2023, Case T-557/20

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

incentivize marketers to invest more in pseudonymised data and foster third party's data sharing while ensuring that individuals' personal data is protected. Additionally, future guidance for anonymization and/or constructing a risk-based test should balance the need for concrete, clear, and precise recommendations and the necessity of exercising some margin of discretion by the controller in applying those recommendations. This is, for instance, reflected in the recently adopted ISO Standard on data de-identification which, rather than adopting an impossible zero-risk approach, provides a framework to identify various risks and mitigate (instead of nullify) them across the lifecycle of deidentified data.

FEDMA's Recommendations:

EU policymakers and DPAs should:

- Foster common pseudonymisation criteria across the EU through guidelines and Codes of Conduct.
- Incentivise companies in investing resources to process pseudonymous data.
- Adopt a risk-based approach to the concept of anonymous data in light of existing international standards such as ISO/IEC 27559:2022.

VI. DATA CONTROLLERS & DATA PROCESSORS: Preserving a clear and proportionate allocation of responsibilities

The allocation of data controller-processor responsibilities across the data marketing value chain still raises significant legal uncertainty among marketers. Through the attribution of the role, the liability and responsibility for safeguarding the processing of personal data changes as does the ability to exercise control over and determine further uses of the personal data. Though some Business-to-Business (B2B) relationships are rather simple, this is not always the case, especially where there are multiple intermediaries within a processing operation. In this situation, the EDPS guidelines 07/20 have proved to be a useful tool, but some statements from certain DPAs which consider existing controller to processor relationships as joint-controllerships can even force some organisations to cancel specific projects. For example, it is extremely challenging to provide the data subject with the information listed under Art. 14 GDPR where these "new" joint-controllerships arise for existing data, thus some processing must inevitably be given up.

This is reflected in the opinion of German DPAs (e.g. Baden-Württemberg, Berlin) according to which the use of third-party data from list owner of third-party addresses for postal promotion leads to a joint-controllership. These interpretations are thus pushing companies to shield themselves from any infringement risk and extend the controllership in case of uncertainty. As a result, **joint controllership**

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org

is increasingly pushed down the marketing value chain, with companies being made liable also for (potential) mistakes made by their clients. For instance, if an advertiser has an insufficient transparency information, it is going to be made not only the advertiser's fault, but it is also automatically the fault of the marketing service provider acting as a joint controller partner. These situations are thus often challenging for marketing services providers which are often SMEs and - in contrast to large brands – do not have the resources to cover the potential costs stemming from the shared liability of a joint controllership. Accordingly, companies which cannot afford the liability risk are often forced to refuse taking the joint controllership, leading to a loss of potential revenue.

Not only the qualification of data controllers in data and marketing operation is gradually being extended to existing controller to processor relationships, but **some DPAs' opinions seem to increasingly expand the obligations of data controllers beyond the provisions of the GDPR**. The French CNIL, for example, recently held that when relying on consent through contractual commitments of partners, the controller is under the obligation to audit such partners, including in controller to controller or joint controller relationships[11]. Not only this requirement is not provided by the GDPR, but it does also create an unclear interplay between data protection legislation and contract law as even the latter does not require audits to be performed in order for a contract to be considered an acceptable way for the controller to comply with its obligation to obtain consent. This case also points out an increasing tendency by DPAs, as mentioned in Section I, to consider that the GDPR prevails over any other law, rather than promoting a constructive balance between different (but equal) rights.

FEDMA's Recommendations:

EU policymakers and DPAs should:

- Preserve a clear and workable allocation of responsibilities in the value chain.
- Adopt and apply a consistent definition of joint-controllership.

***

[11] CNIL, 29 November 2022, Commercial prospecting and rights of individuals: EDF fined 600 000 euros

Federation of European Data and Marketing
Av. Des Arts 43, 5th Floor, 1040 Brussels
+32 2 779 4268 www.fedma.org