IE – ECIJA DIGITAL LAWOBSERVATORY

Focus Group Report – DATA GOVERNANCE

June 7, 2023

https://www.ie.edu/odigitallaw/

Introduction

On April 12, 2023, the focus group session on data governance and data protection took place as part of the activities of the IE – ECIJA Digital Law Observatory. On this occasion, the participants sought to analyze and discuss the concept and scope of data governance systems as well as some of the main implications, challenges and trends in the field of privacy.

The focus group participants were members of the legal and privacy teams of major companies from various sectors, whose common factor is the importance of data in their business activities. They shared their experiences, knowledge and opinions on data governance systems and the main challenges, needs and opportunities that they have identified through their respective positions.

This report is the result of everything that was shared during this fascinating focus group session.

Data governance systems: concept

It is the set of corporate mechanisms and structures aimed at controlling and managing, with a commercial end goal, all business information, which includes all types of data, not just personal data. This data therefore includes **procedures, people and infrastructures**.

In general terms, its objective is to ensure that corporate data achieves high standards of availability, integrity, security, relevance and usability to allow decision-making, as well as data management consistent with the organization's strategy.

In the words of the Global Data Management Community (DAMA), "*Data governance is defined as the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets. The data governance function guides all other data management functions.*"

It is not difficult to understand the reason why more and more companies are undergoing the revision of their structures and processes to create a data governance system.

Data is an essential intangible asset for any company, making possible everything from the basics—proper business management and informed decision-making—to more mature strategic issues such as digital transformation processes or strategies for the much-desired monetization of data.

Reasons for implementing a data governance system include:

- These systems establish the necessary parameters for the management and use of data in an organization, thereby improving data accessibility.
- Such systems also contribute to an appropriate level of regulatory compliance, especially in terms of information privacy and confidentiality.
- They improve the company's flexibility, as well as its effectiveness and efficiency in terms of costs;
- They contribute to reducing risks of various kinds (strategic, business continuity, legal, reputational, etc.)
- They improve the quality of the data being handled.
- They act as support for the overall strategies of the business model in question.
- They allow for handling data in a way that contributes to the satisfaction and loyalty of internal and external customers;
- They add and protect the value of intangible assets;

Additionally, given the ever-increasing volume of data that companies handle, an absence of management and data governance strategies leads to informational disorganization and chaos, and deprives organizations of the benefits of this management system.

What is needed to implement a data governance system?

- First of all, it's necessary to identify the objective(s) of each company in implementing its data governance system. Only then will it be possible to define the scope, systems, infrastructure and other requirements necessary. While it is true that there are objectives common to any data governance system, each organization will also have its own objectives aligned with its business and commercial strategy, ensuring that information management contributes substantially to achieving these goals.

- The next step is asset inventory. It's necessary to identify the databases present in the organization, their origin, the data systems involved, the way they are used, their purposes, etc. A complete knowledge of the data lifecycle is required to be able to take action to improve it.

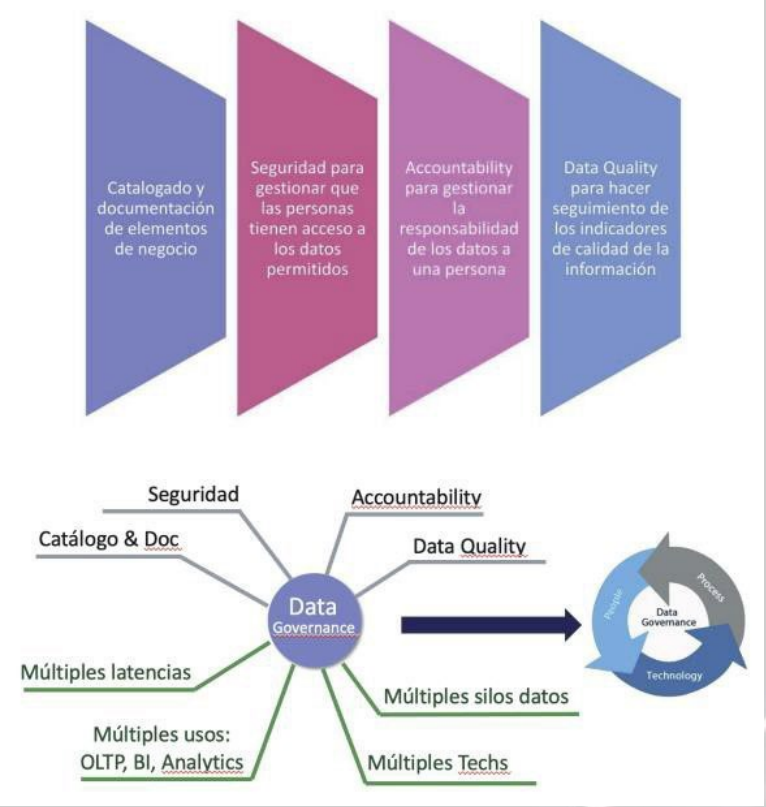
- A data governance system must have policies, processes and roles. It requires a set of well-defined rules and procedures. Some such systems are designed to guide the effective treatment of data and its specifics, e.g., data collection, use, preservation, security and anonymization or transformation processes. Others, like guidelines, are entrusted with making the above rules a reality in the organization via the tools and people involved. Again, all the above policies must be aligned with the organization's strategic objectives; only then will there be coherence between the different guidelines, and data management will contribute significantly to achieving the company's goals.

- For the system to function properly, a human team is essential, with well-defined roles and responsibilities in accordance with their training and experience. The composition of this team will vary from one company to another according to their particular characteristics and needs, usually including positions such as Chief Data Officer (CDO), Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO).

- Technological tools and architecture are necessary to support the governance system, enabling information to be stored and managed securely and in a way that allows for managing the complete life cycle of the organization's data. Information management systems are key to facilitating orderly, agile and flexible data management. They are also the key to improving data quality, optimizing data use and enabling data reuse. It is therefore necessary to identify and describe them in detail to then verify whether the selected structure or applications allow the organization to manage the data in accordance with the defined purposes and procedures.

- It will be necessary to set up a monitoring and control system. This allows for verifying that the policies designed are implemented successfully, and it also enables us to measure the impact that the implementation of the data governance system has on our organization. To measure this impact, it will be necessary to define the relevant ratios or KPIs for each organization.

- As in any improvement process of this nature, there is an enormously relevant cultural factor that must not be overlooked. Training and awareness regarding the value of data as an asset will help members of the company to understand and contribute to the implementation and maintenance of the system.



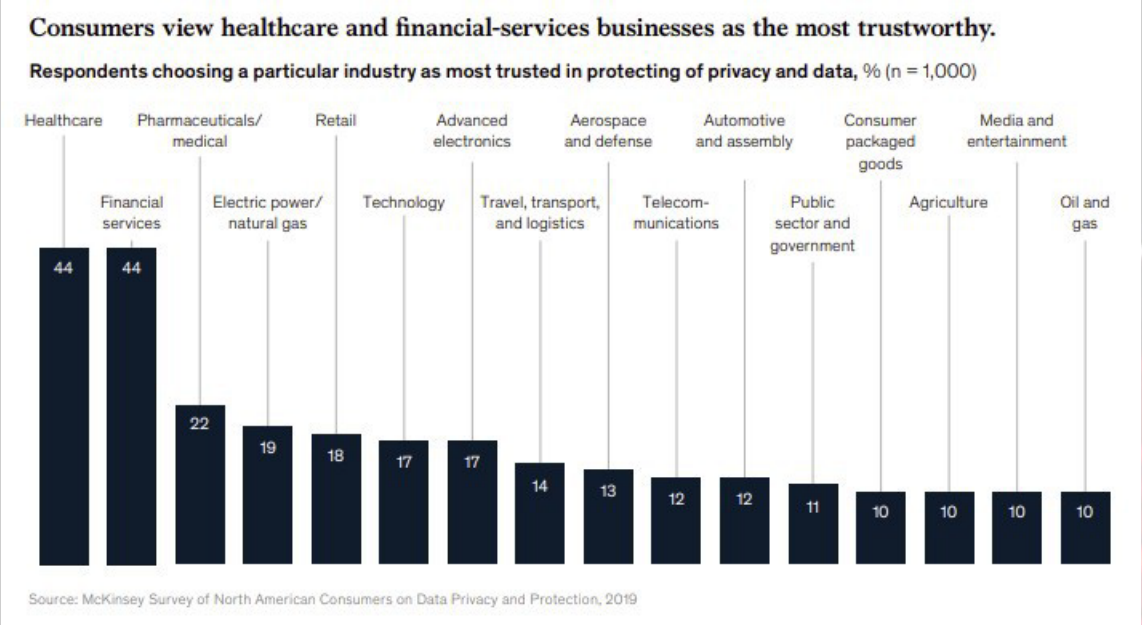
Source: Graph Everywhere

Although it's true that it's difficult to access reliable and up-to-date information that helps to measure the business sector's investment in or commitment to these systems, it is undeniable that, in recent years, it has become increasingly important and beneficial to have a suitable data governance system, particularly in view of several factors:

- ✓ The increase in the amount of data that companies are able to generate. This is so much the case that the European Union estimates a 530% increase in the volume of data worldwide by 2025 (from 33 zetabytes in 2018 to 175 zetabytes).

- ✓ The concern or interest of companies around the world to exploit data efficiently and to monetize its value.
- ✓ The increase in regulatory efforts aimed at both improving information-related risks and creating legal frameworks that promote and foster the data economy. One such example is the Data Governance Act[1] (DGA), a legislative proposal by the European Commission aimed at promoting the data economy and encouraging the exchange, circulation and availability of data between the public and private sectors, with obligations enforceable as of September 2023.

In addition, there are certain sectors that are especially receptive to the adoption of a data governance system because of either the volume or sensitivity of data they handle, as well as the regulatory framework to which they are subject, such as the technology sector, the banking sector or the health sector.



Source: McKinsey

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022, on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

However, in Europe, there is a high-impact regulatory framework common to all companies, for which it is extremely useful to have a data governance system in place: the General Data Protection Regulation (GDPR). [2]. Privacy-related matters are therefore particularly relevant when talking about data governance, and a number of privacy concerns were discussed in the focus group that produced this report.

Monetizing the asset

When discussing information management and exploitation, there are several matters that companies are concerned about, such as the monetization of this information and the presence of ethical principles in its processing framework.

In today's data-driven economy, it is clear that the main focus of any company regarding the data at its disposal is commercial and economic in nature. Data is one of the most valuable intangible assets for many companies, and their efforts are focused on increasing its value and monetizing it. This data monetization can be direct or indirect.

The ability to achieve indirect monetization of data is closely linked to this data's ability to contribute to the company's strategic objectives. The possibilities in this regard are wide-ranging:

- Proper information management contributes to improved decision-making so that decisions lead to actions that improve the efficiency of the organization.
- It also allows for broader knowledge of the target, which will facilitate the improvement of the product or service.
- It helps to better steer the company's commercial strategy and to differentiate the company from its competitors.
- It contributes to reducing business costs and risks;
- It can even play a role in building corporate reputation and trust.

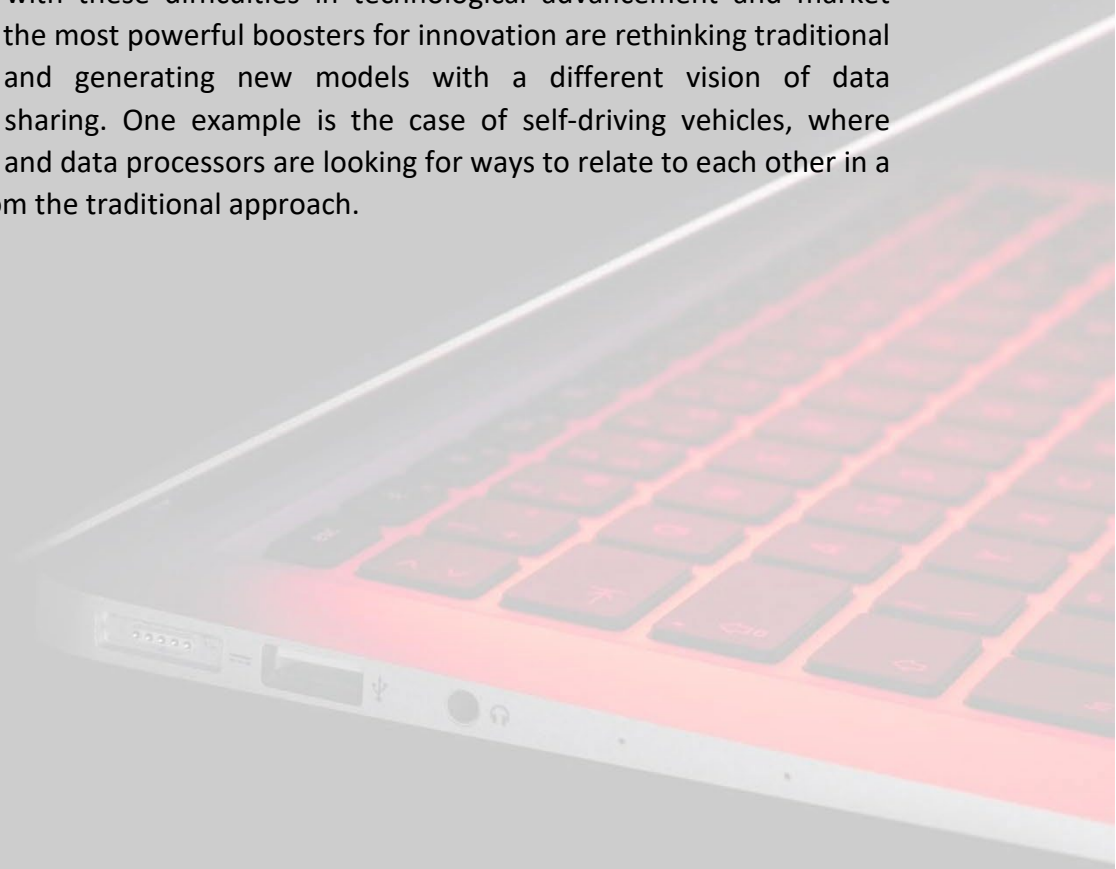
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

However, formulas for direct monetization of data, i.e., formulas capable of providing a direct economic benefit, are the ones that attract the most attention from the business sector. However, when personal data is involved in these processes, the principles imposed by the GDPR regarding the need to have specific consent for each purpose—as well as the principle of data minimization—limit the possibilities, especially if these operations involve other companies or stakeholders.

Beyond operations such as the sale of intangible assets associated with a company or branch of activity, there are also regulatory barriers surrounding the possibility of selling or licensing data. Hence, anonymization, pseudonymization, masking, "noise" generation and other such techniques are front and center for many companies and are incorporated into the data lifecycle in data governance systems, in order to ensure compliance with the GDPR and thus protect the rights of data subjects.

These are not only effective security measures in privacy management, but also—especially anonymization and pseudonymization techniques—the gateway to data sharing and open data projects.

Once again faced with these difficulties in technological advancement and market dynamics, some of the most powerful boosters for innovation are rethinking traditional business models and generating new models with a different vision of data management and sharing. One example is the case of self-driving vehicles, where different data silos and data processors are looking for ways to relate to each other in a way that differs from the traditional approach.



Data products are similar to consumer products in many ways.

Examples of similarities

	Digital product *Example: Computer app*	**Physical product** *Example: Car*	**Data product**
Product features			
Customization of base product for different users	App enables users to personalize the layout, color schemes, and content displayed and to select plans and pricing structures that meet their needs	Car buyers may purchase a variety of special options (eg, leather upholstery, tinted windows, antitheft systems)	Data products can be wired to support different systems that consume data, such as advanced analytics or reporting systems
Delivery of regular product enhancements	Automatic downloads of new functionality	New models Engine modifications that boost fuel economy	New data Support for additional consumption archetypes
Production efficiency			
Reuse of existing processes, machinery, and components	Software developers reuse blocks of code	Automakers use a common chassis on vastly different cars	Organizations reuse blueprints and modular technologies for consumption archetypes across products

Source: McKinsey

Another issue that is often debated among privacy-sector players is the rigidity of the European legal system compared to the American system, which is much more innovation-oriented. This is despite the fact that the GDPR itself states that it does not aim to become an obstacle to personal data processing but rather to create an environment of security that facilitates data flow and the economic progress of the European region.

There are several underlying reasons for the differences in these systems. While the American system is more economy-oriented and gives greater priority to national security, the European system is more focused on social rights and gives priority to guaranteeing these rights. There are also cultural reasons involved; the concept of privacy, itself subjective, is not viewed the same way by both systems.

But differences arise not only when it comes to non-EU regulatory frameworks. Another issue that came to light in the course of the work that led to this report is the disparity in how certain issues are interpreted, which can be seen in the various European supervisory authorities' decisions—as well as the difficulties that this entails for the market and innovation. In order to avoid turning the GDPR into a new directive when applying it, one factor that may potentially help is the promotion of the cross-border cooperation tools and mechanisms provided for in European legislation.

Ethical principles in data governance

Tied to the issue of monetization is the question of ethics in the data's use, which arises in the context of the debate on data governance and privacy. It seems that, in the wake of major scandals and sanctions, and due to the presence of technology that increasingly interferes in privacy (artificial intelligence, biometric technology, etc.), the terms "exploitation" and "monetization" of data have acquired a negative connotation. However, as mentioned earlier, one of the main objectives of the GDPR is to create the necessary legal certainty so that data processing can, with due respect for fundamental rights, contribute "to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons." It is therefore necessary to fight against the negative image of data exploitation by promoting ethics among its principles, so that the resulting benefit is not only economic, but also contributes to social welfare and benefit.[3]

Including ethics principles in a data governance system is therefore essential to ensure the responsible, transparent and ethical use of data in an organization. Consequently, more and more companies are identifying and defending the ethical principles they want to promote and are working to integrate them into information management.

To do this, these principles must be duly reflected in the policies and procedures that form a part of the system, incorporating clear guidelines on how to process data with due transparency and respect for the rights of data subjects, which collection and analysis techniques are the most appropriate according to these principles and, most importantly, understanding how the use of data impacts data subjects.

Incorporating a staff profile into the management team, assigning this task to one of the members of the data governance system, most likely to the chief data officer, or even creating an ethics committee to take on this task will contribute to the implementation and respect of these principles. So, too, will the introduction of privacy training and awareness-raising measures in the organization.

It will be helpful in this regard to provide employees with suitable channels for reporting concerns or breaches and to set up monitoring and control systems.

[3] Recital 4. GPDR. "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."

Privacy-related roles

In a data governance system, the responsibility for data privacy is primarily assigned to the chief privacy officer (CPO), who is in charge of ensuring that the system complies with data protection principles and obligations, as well as of establishing privacy-related policies and practices within the organization.

However, despite the fact that five years have passed since the GDPR took effect, which assumes a certain maturity in terms of its application, there is a recurring theme regarding the correct identification of the roles that can (or should) exist in a company in terms of privacy.

There are still many organizations that, for various reasons, do not identify these roles in accordance with the provisions of the GDPR—which is why we find data protection officers (DPOs) actually performing the duties of chief privacy officers (CPOs) and vice versa—or simply do not have them.

The main reasons for this are a lack of resources and lack of awareness of their relevance. Not all companies can sustain the cost of these roles, especially if several roles are required. Even today, it is still difficult for many companies to correctly distinguish between the role of the DPO and the CPO.

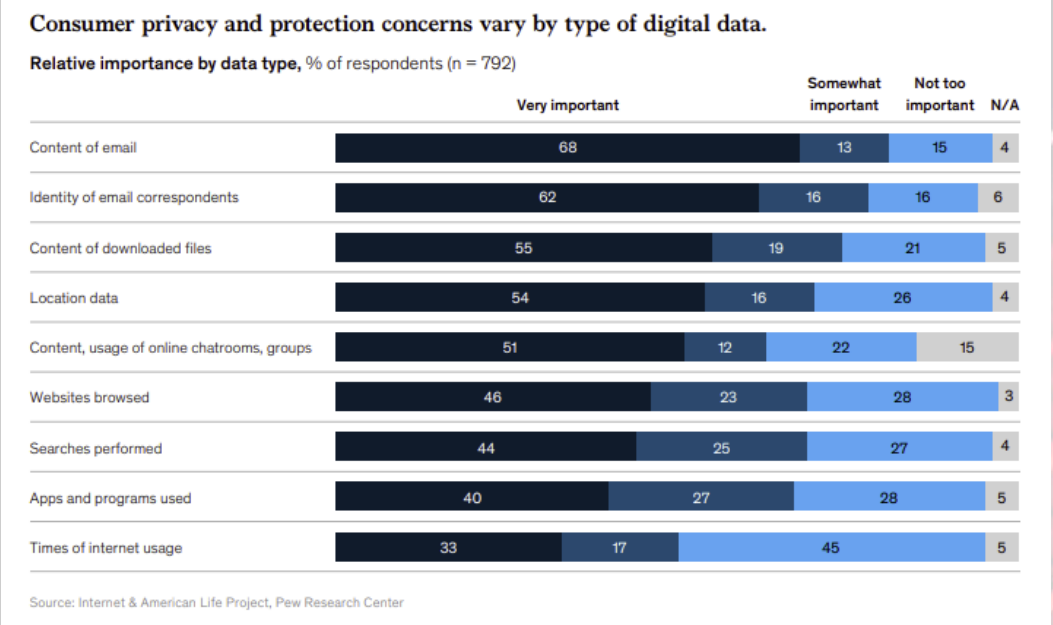
The figure of the DPO, whose origins date back to the German Federal Data Protection Act of 1977, has always played a supervisory role in relation to compliance with data protection regulations. The GDPR recovers this role and provides it with specific characteristics (independence, qualification and position in the company) and functions. The role of the CPO has a broader vision of privacy in the organization that includes ethical, strategic and operational aspects. It is therefore the main role in terms of privacy within the framework of the data governance system.

Following on from the supposed maturity (or lack thereof) of the business ecosystem in terms of GDPR compliance mentioned above, the sector detects the need for greater and improved awareness of the impact of privacy in any company and the need to provide companies not only with the necessary roles, but also with sufficient resources to achieve this.

Superficial compliance is still too widespread, often based on the fear of a sanction from the corresponding control authority, as is reactive compliance (i.e., compliance triggered by the filing of a disciplinary action or following the aftermath of a security breach).
The industry is calling for greater awareness of the need to create and properly scale the structures necessary to ensure compliance with privacy regulations, but, above all, awareness of the positive relevance and impact that this has for any company.

Measures such as those contained in Directive (EU) 2016/1148 of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union (known as NIS2), although aimed at the field of cybersecurity rather than privacy, seem likely to help engage organizations' senior management positions, as this directive establishes sanctions specifically targeted at management for certain cases of non-compliance.

Consumers' growing concern about their privacy and the increase in the number of complaints[4] they file with supervisory authorities is undoubtedly another factor that may help improve the level of awareness in the business sector.



Source: McKinsey

[4] According to the 2022 report from the Spanish Data Protection Agency (AEPD), there is an upward trend in the number of complaints, "with an increase of 9% compared to 2021 and 47% compared to 2020."

Growing trend toward delegated security environments

In conversations about data governance, when the topic turns to the information infrastructures and systems needed to make governance possible, unavoidable issues arise, such as the tendency to resort to external providers, thus increasing the use of what are known as delegated security environments, and the concern about the security of these environments, given the steady increase in security breaches.

Delegated information security environments refer to those in which an enterprise relies on an external provider, such as a Managed Security Service Provider (MSSP) or cloud service provider, to manage and/or maintain the security of its data and systems.

The steady growth of reliance on this type of provider stems from a variety of reasons, including:

- Primarily, reduced investment in information management and security infrastructure. Outsourcing such services to a third party is usually significantly cheaper for a company than performing them itself, and these services are offered on more affordable pay-as-you-go or subscription models.

- Having an external provider allows the company to benefit from the provider's experience and qualified knowledge in designing, implementing and managing security solutions, as well as in detecting and responding to security incidents. In addition, most providers already have certifications that allow the company not only to save on the cost of acquiring these systems, but also to certify their soundness to third parties.

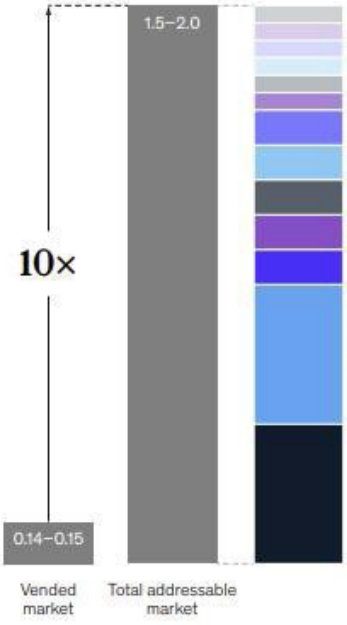
- The flexibility that MSSPs offer in adapting and customizing their products to specific customer needs is, without a doubt, another of their added values. They are also in a constant process of improvement, relieving the customer of this task.

- Their expertise in providing these services and the resources they have at their disposal make them more effective in identifying security threats and responding to any incidents.

The services of an external provider can therefore provide the company with specialized, mature and continuously improving systems.

The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, $ trillion



Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

Source: McKinsey

However, it is the company's legal obligation, as data controller or data processor, to select service providers that offer sufficient guarantees; thus, one of the issues of greatest concern to the business sector at this time is the exercise of due diligence in its relationship with these third parties.

In order to do so, companies are not only faced with the need to implement verification and diligence measures at the time of selection, but they must also design specific procedures that allow them to maintain this diligence throughout their relationship with the provider, measures that must adapt to each type of provider and to the specific characteristics of the data processing being carried out.

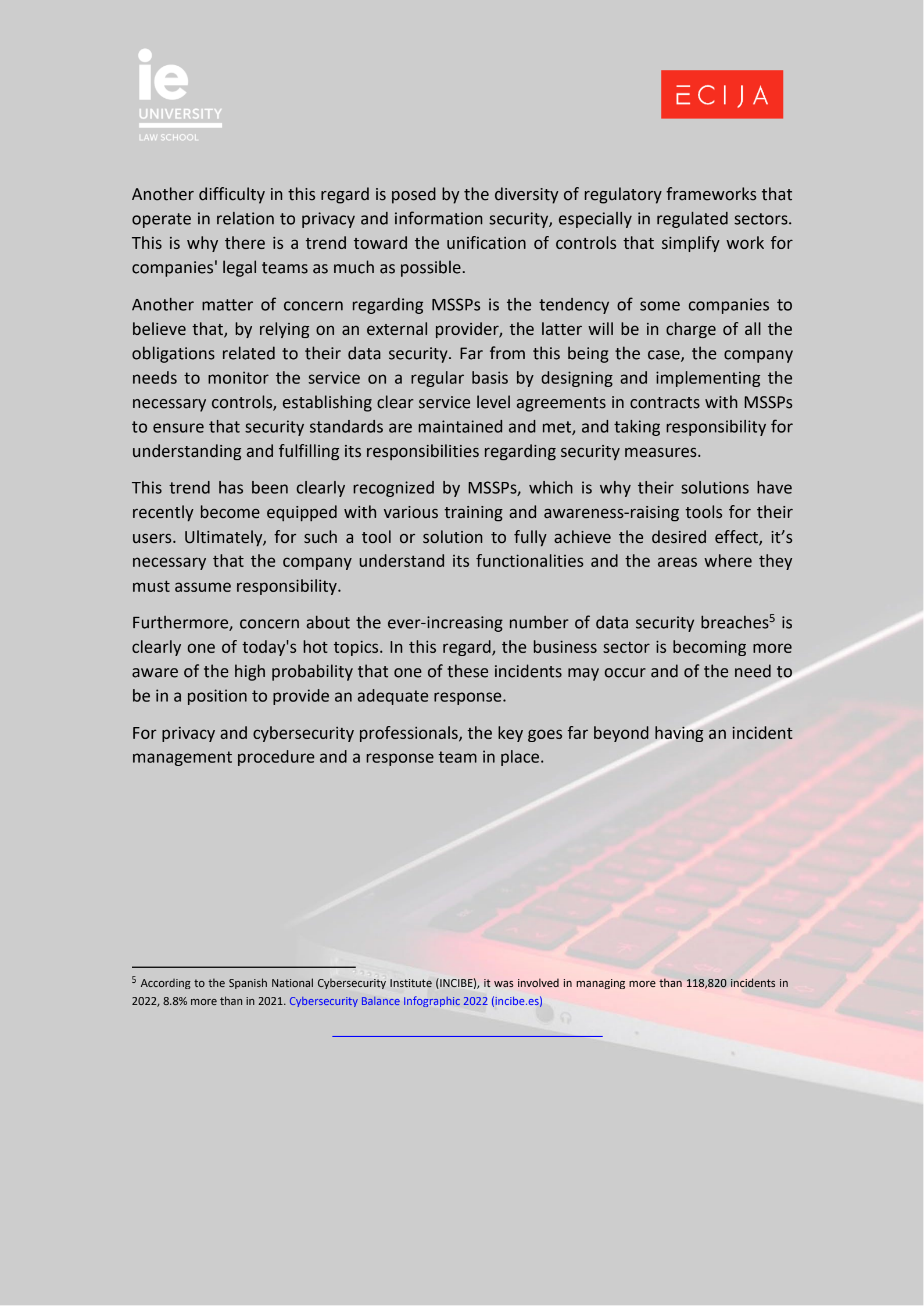
Another difficulty in this regard is posed by the diversity of regulatory frameworks that operate in relation to privacy and information security, especially in regulated sectors. This is why there is a trend toward the unification of controls that simplify work for companies' legal teams as much as possible.

Another matter of concern regarding MSSPs is the tendency of some companies to believe that, by relying on an external provider, the latter will be in charge of all the obligations related to their data security. Far from this being the case, the company needs to monitor the service on a regular basis by designing and implementing the necessary controls, establishing clear service level agreements in contracts with MSSPs to ensure that security standards are maintained and met, and taking responsibility for understanding and fulfilling its responsibilities regarding security measures.

This trend has been clearly recognized by MSSPs, which is why their solutions have recently become equipped with various training and awareness-raising tools for their users. Ultimately, for such a tool or solution to fully achieve the desired effect, it's necessary that the company understand its functionalities and the areas where they must assume responsibility.

Furthermore, concern about the ever-increasing number of data security breaches[5] is clearly one of today's hot topics. In this regard, the business sector is becoming more aware of the high probability that one of these incidents may occur and of the need to be in a position to provide an adequate response.

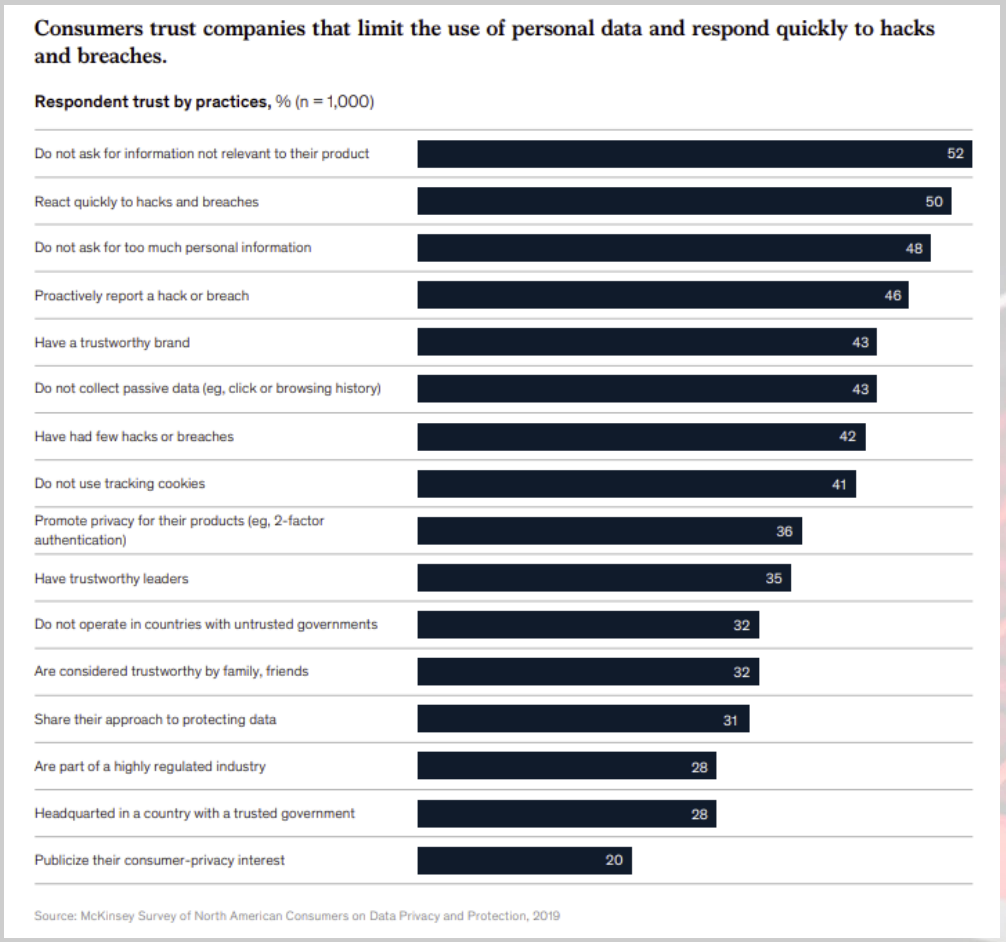
For privacy and cybersecurity professionals, the key goes far beyond having an incident management procedure and a response team in place.



[5] According to the Spanish National Cybersecurity Institute (INCIBE), it was involved in managing more than 118,820 incidents in 2022, 8.8% more than in 2021. Cybersecurity Balance Infographic 2022 (incibe.es)

A security breach is a moment of crisis for an organization. This means that, in addition to procedures or contingency plans that take into account controls regarding privacy, security, business continuity, technical and legal equipment, it is also necessary to have:

- A holistic approach to the incident, taking business and reputational issues into account.
- Prior preparation and testing so that the urgency and surprise inherent in crisis environments does not have a detrimental effect on successfully managing the incident.
- Measures designed and implemented for monitoring and measuring results in order to convert the resilience phase of this type of incident management into a process of continuous improvement.



Source: McKinsey

Meanwhile, the business sector is also drawing attention to the utility that artificial intelligence (AI) tools seem to be demonstrating in managing security breaches.

AI can be useful in identifying, detecting and responding to security breaches, improving speed and efficiency. AI can:

- Analyze large volumes of data with great agility.
- Detect suspicious user behavior patterns because they are different from the usual learned patterns.
- Contribute to more effective detection of malicious activities and incidents.
- Improve incident response through automation.
- Improve digital forensic analysis following security breaches, contributing to organizational resilience.

However, having AI-equipped tools does not exempt companies from employing highly skilled and experienced cybersecurity personnel. In fact, it is the combination of both factors that will facilitate getting the most out of the tool and make it possible to take a prudent and diligent approach, given the challenges associated with using AI (biases in algorithms, ethics, etc.).

Conclusions

The current data economy and the road travelled since the GDPR took effect have afforded us maturity in data management and, most importantly, objectives to pursue. However, the reality is that this degree of maturity can still be perfected; in fact, it must always be addressed within the framework of a continuous improvement process.

The implementation of data governance systems is proving to be a way to achieve this maturity, allowing companies to manage data with agility, flexibility and security, in alignment with their business strategy, and in such a way that the organization can begin to perceive these systems and the resources involved in them as an investment and an opportunity.

Procedures, people and infrastructure are the keys to building these systems. As with any change process, a cultural change is required in the organization in which privacy professionals play a strategic role, while it is also true that greater awareness and involvement of management teams is required to take data protection and security compliance to the next level of maturity.

Acknowledgments:

The following professionals have participated in the IE – ECIJA Digital Law Observatory focus group:

- Marta Duelo, Chief of Legal & Contractual Services at Mobile World Capital
- Marcos García-Gasco, Associate Legal Director (DPO Europe) at Xiaomi
- Ana Regidor, Chief Privacy Officer at Amadeus IT Group
- Borja Larrumbide, Security Assurance for Spain and Portugal at Amazon Web Services
- Mireia Martínez, Head of Legal, International & Data Privacy at Glovo
- Miguel Álvarez, Corporate Counsel & Head of Legal at Canon
- Macarena Rosado, General Counsel at IE University

In this report, participants shared their experiences, knowledge and opinions on data governance systems. These opinions are the author's responsibility and do not necessarily represent those of the company.