IE – ECIJA DIGITAL LAW OBSERVATORY

CYBERSECURITY Focus Group Report

October 26, 2023

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

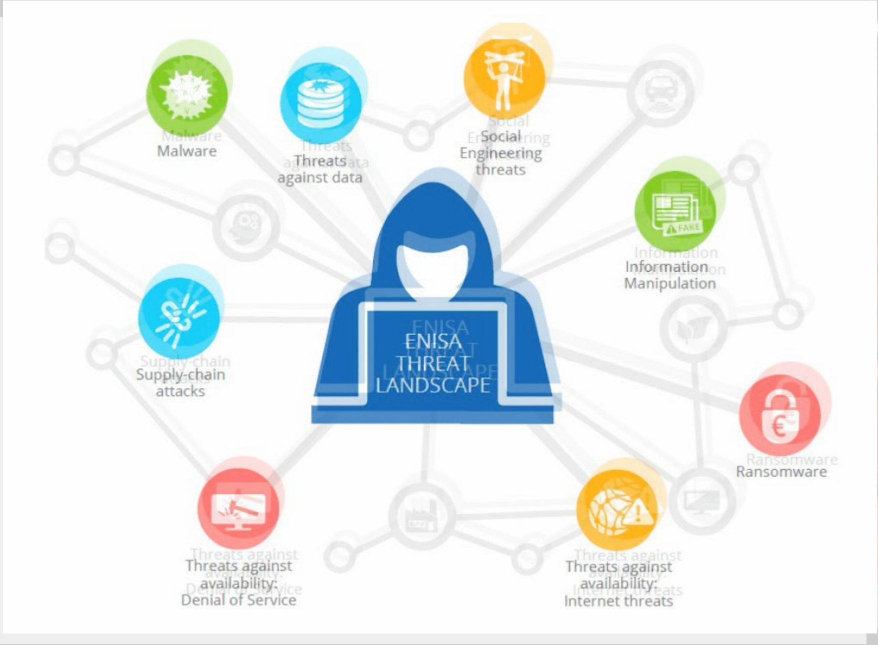
Intruduction

On October 26, 2023, a working session or Focus Group on Cybersecurity was held as part of the activities of the IE-ECIJA Digital Law Observatory. The participants' objective was to analyze and discuss the European strategy on cybersecurity, specifically focusing on the regulatory developments in recent years and the expected developments in the coming months.

The participants of the Focus Group, members of legal, privacy, and cybersecurity teams from major companies belonging to various sectors, whose common factor is the relevance of cybersecurity in their activities, shared their experiences, knowledge, and opinions on this topic, as well as the main challenges and needs/opportunities they identify from their respective positions. This report is the result of everything shared during the working session.

Regulatory development within the framework of the European Cybersecurity Strategy

In recent years, there has been a worrying increase in the frequency and magnitude of security breaches worldwide. Reports from various sources such as ENISA (European Union Agency for Cybersecurity) indicate that these breaches have experienced exponential growth, affecting millions of individuals and businesses. Over the past five years, there has been an increase of over 300% compared to previous periods. These breaches have not only affected large corporations but have also impacted small and medium-sized enterprises, highlighting the breadth of this threat.


Malware
Threats against data
Social Engineering threats
FAKE
Information Manipulation
Supply-chain attacks
ENISA THREAT LANDSCAPE
Ransomware
Threats against availability: Denial of Service
Threats against availability: Internet threats

Fuente: ENISA THREATS LANDSCAPE 2023

Europe, aware of this reality, has implemented a Cybersecurity Strategy1 that reflects its commitment to digital protection. This strategy has resulted in the emergence of various standards focused on protecting different aspects over the past year:

- CER Directive: Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, focused, as its name indicates, on the resilience of critical entities.

- NIS2 Directive: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (SRI 2 Directive): This directive focuses on harmonizing cybersecurity aspects in entities deemed essential and important in the European Union. Its transposition into Spanish legislation, expected to occur before October 2024, will have a significant impact on various sectors such as Energy, Transportation, Banking and financial markets, Insurance, Healthcare, laboratories, research, Drinking water, waste management, Digital infrastructure, Managed ICT services, Space, Public administration, Manufacturing, production, and distribution of chemicals, Postal services, Food: Production, distribution, and transformation, Manufacture of vehicles and transport equipment, Manufacture of medical devices, Manufacture of computer, optical or electrical products, and Digital service providers.

- Dora Regulation: This regulation (Digital Operational Resilience Act) focuses on strengthening the digital operational resilience of credit institutions, payment institutions, electronic money institutions, investment firms, insurance undertakings, and ICT service providers. Already in force, its obligations will begin to take effect in January 2025.

- Cyber Resilience Law: This is a proposal by the European Commission to strengthen cybersecurity standards and ensure the security of hardware and software products in the European Union. The law establishes mandatory cybersecurity requirements for manufacturers and retailers of digital products, such as wireless and wired products and computer programs. Additionally, the law increases the liability of manufacturers by requiring them to provide security support and software updates to address detected vulnerabilities. Consumers will also have access to sufficient information about the cybersecurity of the products they purchase and use.

- Certification Schemes by ENISA: The European Union Agency for Cybersecurity (ENISA) has developed three new European schemes under the Cybersecurity Act: The European Cybersecurity Certification Scheme based on Common Criteria (EUCC), the European Cybersecurity Certification Scheme for Cloud Services (EUCS), and the EU Cybersecurity Certification Scheme for these three certification schemes are expected to be of great importance in the future within the European framework, particularly regarding 5G networks.

[1] https://digital-strategy.ec.europa.eu/

The Focus Group primarily focuses on the NIS 2 Directive and the Dora Regulation. Both regulations are shaping up to impact a wide range of sectors. Their implementation within entities requires a significant effort to adapt to the new regulatory requirements aimed at safeguarding the integrity of information and operations in an increasingly challenging cybersecurity landscape.

During the meeting, concerns are expressed regarding the decision to keep NIS 2 in Directive format, despite the perceived "failure" associated with NIS 1. The question of why NIS 2 has not adopted the form of a Regulation, similar to DORA, arises from the suspicion that the situation experienced with its predecessor may be repeated. The fact that NIS 2 continues as a Directive poses the evident risk that individual transposition in each member state may not be sufficient to achieve the objectives intended by this regulation, a homogeneous regulation.

Transformation of Cybersecurity into a Central Element of Corporate Governance

The growing relevance of cybersecurity has transformed its nature, transcending merely technical or technological aspects to become a crucial element for entity governance. This paradigm shift demands active participation from senior management and the legal department in formulating strategies to safeguard organizational integrity. In this new context, cybersecurity entails a cultural change where the creation of new processes and scenario planning becomes imperative for an effective response to crisis situations, considering the exponential increase in cyber-attacks. In this new landscape, digital security is not solely the responsibility of the technology team but is integrated into executive and legal decision-making.

Close collaboration between technical and legal departments is essential for comprehensively addressing cybersecurity challenges.

Specialized Cybersecurity Committees with a Mixed Focus

Given the complexity of cyber threats, many entities opt to establish specialized cybersecurity committees. These committees not only involve technical and security experts but also incorporate legal teams. The presence of these profiles allows addressing challenges from complementary perspectives, ensuring a comprehensive understanding of both the technical and legal aspects associated with cybersecurity.

The collaboration among technical, security, and legal professionals in these committees not only enhances incident response capabilities but also facilitates the formulation of policies and strategic decision-making. The diversity of skills and knowledge in these mixed teams contributes to the creation of more robust and effective cybersecurity strategies.

Shortage of Cybersecurity Professionals in the Legal Field

As the importance of cybersecurity in corporate governance grows, the critical need for specialized talent in cybersecurity within legal teams arises. Currently, finding professionals who possess both legal skills and deep cybersecurity knowledge is a significant challenge in the job market.

The solution to this talent shortage involves proactively identifying and recruiting individuals who can integrate these dual skills. Organizations and institutions must invest in training and development programs to equip legal professionals with specific cybersecurity knowledge. Additionally, creating networks and collaborations with specialized academic institutions can be crucial in fostering the training of professionals who can effectively address the legal complexities of cybersecurity.

Training for Senior Management in Cybersecurity

Europe is aware that decisions regarding cybersecurity in essential and important entities are crucial, so it establishes in the NIS 2 Directive, pending transposition in our country, the need for senior management to receive specific training in this regard. Training senior management in cybersecurity not only involves understanding threats and associated technologies but also understanding how these affect the company at a strategic and financial level. Training can address topics such as cyber risk management, establishment of security policies, and understanding the legal implications associated with cybersecurity risks. This proactive approach not only strengthens the decision-making capacity of senior management but also contributes to a more aware and committed organizational culture towards cybersecurity, which ultimately is one of the main objectives of the European Cybersecurity Strategy.

In fact, it is crucial to indicate that NIS2 Directive itself establishes direct responsibilities for Senior Management in Article 32 regarding cybersecurity, indicating that in case of non-compliance with the Directive "... Member States shall ensure that competent authorities are empowered to: request that the courts temporarily prohibit any person exercising management responsibilities at the level of CEO or legal representative in such essential entity from exercising management functions in said entity. Member States shall ensure that any individual responsible for an essential entity or acting as its representative, making decisions on its behalf, or exercising control over it, has competencies to ensure compliance with this Directive.
Member States shall ensure that such individuals can be considered "responsible for failing to ensure compliance with this Directive."

RGPD Vs NIS

In the Focus Group, it is highlighted that cybersecurity should not be confused with the protection of personal data, although both concepts are interconnected in certain aspects. The main difference lies in their approaches and objectives, being regulated by different regulatory frameworks.

The GDPR primarily focuses on protecting privacy and individual rights in the processing of personal data. It establishes clear principles regarding the collection, processing, and establishment of security measures for personal data, ensuring that organizations manage data ethically and respectfully. On the other hand, cybersecurity regulations such as NIS2 and DORA focus on safeguarding entity information, securing the systems and digital infrastructure they depend on. These regulations establish measures and practices to prevent, detect, and respond to security incidents. In this context, the aim is to protect not only personal data but also the entirety of an entity's digital infrastructure, safeguarding the entity's business data.

Although the objectives of these regulations are different, as previously indicated, there is a convergence in establishing security measures based on risk. However, these risks can be very different in each case.

This distinction is important when establishing by contract the security measures that must be implemented by a service provider, as it is crucial to differentiate the necessary security measures for processing personal data from the measures necessary to secure the infrastructure and business data.

Risk Management Approach

The main purpose of European cybersecurity regulations is to promote business awareness of cyber risks and encourage the adoption of appropriate measures to ensure information security. In this regard, these regulations seek for companies not only to recognize the importance of cybersecurity but also to understand the need to proactively manage the risks associated with their critical processes.

One of the key elements to achieve this goal is the conduct of adequate risk analysis. Companies must carry out detailed assessments that identify and quantify potential risks to information security. These analyses should not only cover internal threats but also external ones, considering factors such as the nature of the data handled, the technological infrastructure used, and the potential impacts on business continuity.

It is relevant to highlight that these risk analyses may require the involvement of third parties, especially in situations where the supply chain and suppliers play a significant role in the entity's processes. Assessing the risk of suppliers is crucial, as the information security of an entity can largely depend on the security practiced by its suppliers. The risk of a supplier can, in many cases, act as a determining factor in understanding the overall risk faced by the entity subject to cybersecurity regulations. The interconnection between companies and their suppliers necessitates comprehensive risk management. Regulations aim for companies to adopt a holistic approach, considering not only their own systems and practices but also the security of those with whom they are contractually linked.

Information Flow between the Public and Private Sectors

During the meeting, the essential importance of strengthening the exchange of information in the field of cybersecurity between the public and private sectors is highlighted. While there is currently an obligation to report security incidents to regulatory authorities, and on the other hand, CSIRTs have information channels, there is a perceived need to establish a more robust and bidirectional flow of information. This bidirectional approach not only implies that companies report incidents to the competent authorities but also involves authorities proactively sharing relevant information with the private sector more effectively.

The idea of facilitating greater information flow in both directions is based on the premise that cybersecurity is a collective effort. Both government entities and private companies possess valuable information that can significantly contribute to strengthening national and European cyber resilience. Authorities can provide intelligence on large-scale threats, while companies can offer information on specific attacks, patterns of suspicious activity, and sectoral vulnerabilities.

The ease and speed of information exchange are considered crucial elements in improving the response capability to cyber-attacks. Establishing platforms or mechanisms that allow for secure and real-time information sharing between the public and private sectors is seen as a key strategy. This not only streamlines the response to threats but also contributes to building a more resilient and collaborative society in the field of cybersecurity.

Securing the Supply Chain

The implementation of regulations such as NIS2 and DORA triggers a series of significant effects on the supply chain, extending cybersecurity compliance obligations beyond critical, essential, or important entities. This approach not only imposes direct responsibilities on the entity but also requires a duty of diligence in selecting the supply chain, affecting suppliers and service providers. This extension of compliance not only has advantages but also poses challenges.

Advantages of the Chain Effect:

- Improved Resilience: By enforcing supply chain security, there is a widespread improvement in cybersecurity resilience. This contributes to creating a safer and more robust environment, as service providers are often a point of entry for cyber threats.

- Coherence in Security: Compliance requirements for suppliers ensure greater coherence in cybersecurity practices throughout the supply chain. This is essential to prevent weaknesses at any point that could be exploited to compromise overall security.

Challenges of the Chain Effect:

- Financial Burden for Small Suppliers: Smaller and specialized suppliers, which may be crucial for an entity, may face financial difficulties in meeting the obligations demanded by their clients. The costs associated with implementing advanced security measures can be challenging for companies with limited resources.

- Perception of the Legal Department (or Committee) as a Paralyzing Department: It must be avoided that business stakeholders perceive legal cybersecurity as a hindrance. Ensuring effective implementation of security measures in negotiations with suppliers is essential. Currently, negotiations around cybersecurity are often slow and complicated, resulting in delays in hiring necessary suppliers for the entity. However, it is crucial to highlight that ensuring consistency in supplier cybersecurity is an urgent need, and this should be clearly and bindingly reflected in contracts.

  Training business stakeholders is essential to prevent cybersecurity from being perceived as a barrier. Cybersecurity is not only a legal requirement; it is a strategic component for business continuity and asset protection, and therefore, business stakeholders must understand that these measures are not only intended to comply with regulations but also pursue a more important goal, strengthening the entity's competitive position and resilience.

  The consideration of cybersecurity management has become a fundamental and indispensable element when evaluating a new supplier, establishing a significant change in selection processes in purchasing departments. Requesting detailed information about a supplier's cybersecurity practices, security measures implemented, etc., has become common during selection processes and is expected to grow in the coming months due to this chain effect. This proactive and due diligence approach not only reflects the growing awareness of cybersecurity risks but also demonstrates its recognition as a critical factor in business decision-making.

In this regard, it is also important to note that DORA, for its obligated entities, establishes specific requirements that must be mandatory in the client-provider contractual relationship. Among these requirements, we find the following:

- Description of all services provided by the supplier, indicating if subcontracting is allowed and the applicable conditions for such subcontracting.
- Countries and location of the service data storage, including notification in case of changes.
- Provisions on specific security measures related to availability, authenticity, integrity, and confidentiality.
- Guarantees for the client entity to access and easily recover information.
- SLAs (Service Level Agreements) including their updates and revisions; with specific quantitative and qualitative performance objectives.
- Obligation of the provider to provide assistance to the financial entity at no additional cost, or at a predetermined cost, when a ICT incident occurs, establishing specific commitments on notification deadlines and the expected content of that notification.
- The obligation of the provider to fully cooperate with competent authorities.
- Termination rights and minimum notification periods for the termination of contractual agreements.
- Participation of suppliers in ICT security awareness programs and training activities on digital operational resilience of entities.
- Obligation for the provider to participate and fully cooperate in threat-based penetration testing of the financial entity.
- The right to continuous monitoring of the provider's performance including unlimited rights of access, inspection, and auditing by the entity or a designated third party, as well as by the competent authority.
- Exit strategies, in particular the establishment of a sufficient mandatory transitional period to allow migration to another provider or service provider.

In the context of securing the supply chain, auditing suppliers in terms of cybersecurity is fundamental to ensure the integrity and reliability of the supplied services and products. Beyond simple technical assessment, it is essential to analyze the maturity of suppliers in their cybersecurity management. This broader approach involves evaluating how security policies, practices, and processes are integrated into the client's organizational culture.

Identifying specific weaknesses in the cybersecurity of suppliers is a crucial step. It is not only about detecting technical vulnerabilities but also assessing the effectiveness of risk management practices and incident response protocols through clear and transparent corrective actions for both parties. The client must be aware of the execution of these corrective measures by the provider, with specific implementation dates to effectively manage their own risk. It is estimated in the meeting that these supplier assessments or analyses should be carried out approximately every two years at most.

In the realm of risk management, one of the most effective exercises to conduct with suppliers or service providers is the recurrent performance of penetration tests, also known as pentesting. This exercise involves simulating controlled cyberattacks on systems supporting critical processes. By conducting pentests periodically, potential vulnerabilities can be identified and proactively addressed before they can be exploited by external threats, both in the provider's infrastructure and the client's own infrastructure.

Ultimately, the meeting reinforces the idea that closer communication between the client and the provider regarding cybersecurity reflects the importance of building a strong and collaborative relationship in an increasingly complex digital environment. Cybersecurity cannot be effectively addressed as a unilateral concern; it requires a joint effort. In this regard, greater transparency between both parties becomes a fundamental pillar. The client must be fully informed about the security practices implemented by the provider, while the provider must understand the specific expectations and security needs of the client. This transparent and proactive exchange of information not only strengthens mutual trust but also enables a faster and coordinated response to potential cyber threats. Open communication and transparency thus become key elements in building a joint cybersecurity defense, where both parties actively and continuously contribute to the security of the legal relationship and the integrity of the supply chain.

The future of cybersecurity regulations in other countries

In the realm of cybersecurity regulations worldwide, during the meeting, a "Brussels effect" is anticipated, especially in Latin American countries. This term refers to the influence that European regulations, in this case, the NIS2, DORA, and CER regulations, could have as a model for other countries that have not yet established solid cybersecurity regulations or are in an early stage. Similar to the trajectory followed by the General Data Protection Regulation (GDPR) in recent years, it is expected that these European standards will serve as a reference for the development of more robust and updated regulations elsewhere in the world.

This phenomenon not only reflects the growing global importance of cybersecurity but also the need for consistent standards to address constantly evolving digital threats. By adopting regulations similar to NIS2, DORA, and CER, countries could strengthen their positions against the increasing cyber threats, promote similar cybersecurity practices, and provide a more uniform legal framework to protect their infrastructures.

Cyber Insurance

During the meeting, concerns are raised regarding cybersecurity insurance coverage. There is an upward trend in the costs of these insurances, and the requirements for them to provide effective responses to potential losses are becoming increasingly stringent. The rising costs of insurance and the increased demands to activate these policies pose an additional challenge for organizations. They must not only invest in proactive cybersecurity measures but also face significant costs to ensure adequate coverage in the event of a cybersecurity incident.

Cybersecurity incident reporting

The concern about the lack of an effective single point of contact for cybersecurity incident reporting is highlighted as a significant challenge during the discussion. The absence of a centralized point directed to various supervisory authorities (such as AEPD, INCIBE, CCN-CERT) and regulators adds an additional layer of complexity for private entities. The need to make notifications to multiple agencies and within extremely tight timeframes represents a considerable effort for companies, which are already under pressure to contain and manage the impacts of a cybersecurity incident. It implies that private entities must deal with the additional bureaucracy of reporting to various government and regulatory entities, especially in the case of incidents that may impact a multinational operating in different countries. Each of these government and regulatory entities has its own protocols and specific requirements for notification, considering that a thorough assessment of the situation and detailed information collection is required in this type of notification. This temporal challenge may affect the quality of the information provided and potentially hinder an effective response to the incident.

To address this concern, there is a need to establish a harmonized framework that centralizes the cybersecurity incident notification process in a real way. An effective single point of contact would facilitate the task of private entities, simplifying the notification procedure and improving efficiency in managing cybersecurity incidents.

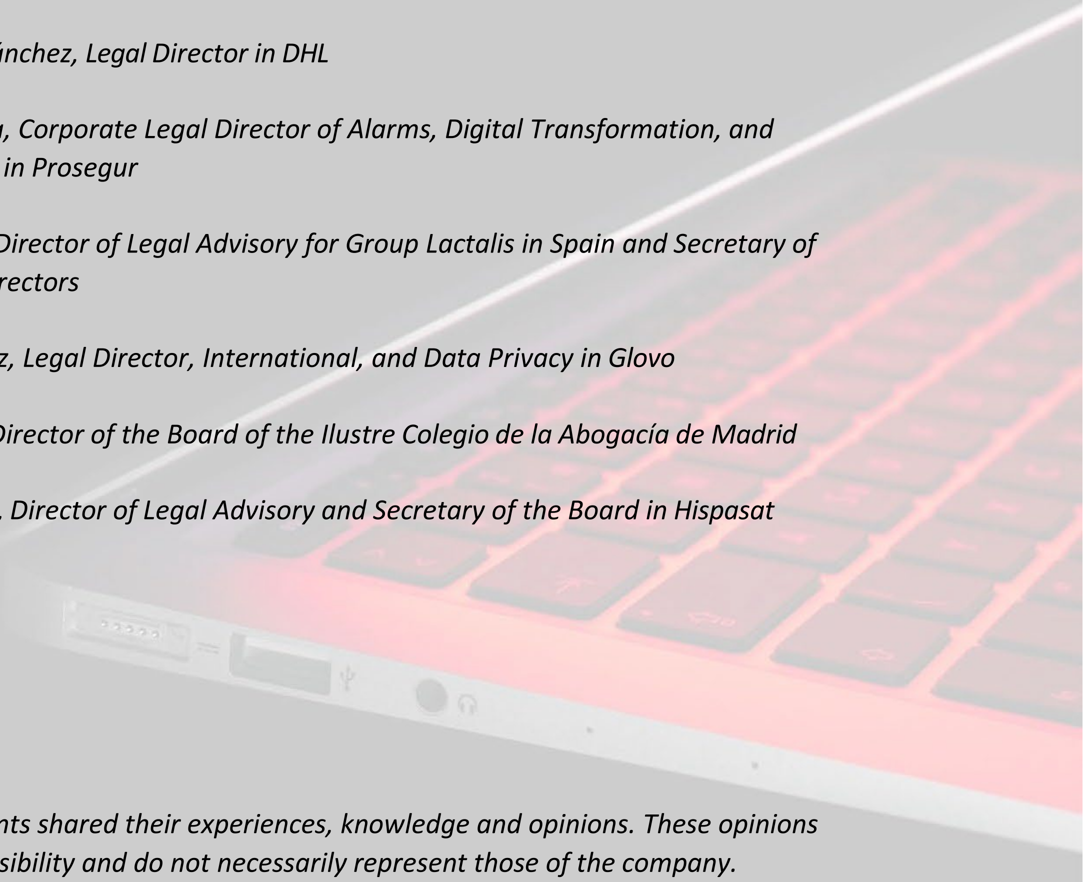
Conclusions

The approval of cybersecurity regulations in Europe, as a result of the Digital Cybersecurity Strategy, marks a significant milestone that presents challenges and opportunities for both entities required to comply with them and their service providers. For entities subject to these regulations, compliance can pose a considerable challenge, as it involves implementing robust security measures, timely incident reporting, and adapting to a constantly evolving legal framework. However, this requirement also presents a unique opportunity to foster greater resilience. By adhering to stricter standards, companies and entities can strengthen their stance against digital threats, reducing the likelihood and impact of potential cybersecurity incidents. Additionally, these regulations act as catalysts for the development of a more ingrained cybersecurity culture in European businesses. By placing renewed emphasis on the importance of digital security fosters awareness and responsibility at all levels of an organization, including senior management. This not only directly benefits entities subject to regulations but also contributes to creating a safer and more reliable business environment in Europe.

Acknowledgments:

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

- *Asier Crespo, Legal Director Microsoft Iberica*
- *Jaime Calvo, Director of Legal, Corporate Litigation, Cybersecurity, Financial Crime Compliance, Security and Intelligence, and Legal Risk in Banco Santander*
- *Juncal Ferrer, Iberia Legal Manager and Privacy Director in JTI Iberia*
- *David Serrano, Director Legal Advisory Litigation in Acciona*
- *Helena Fernández, Legal Corporation Sr. Manager in Repsol*
- *Juan Manuel Sánchez, Legal Director in DHL*
- *Diolimar García, Corporate Legal Director of Alarms, Digital Transformation, and Global Projects in Prosegur*
- *María Cobián, Director of Legal Advisory for Group Lactalis in Spain and Secretary of the Board of Directors*
- *Mireia Martínez, Legal Director, International, and Data Privacy in Glovo*
- *Ana Buitrago, Director of the Board of the Ilustre Colegio de la Abogacía de Madrid*
- *Javier Folguera, Director of Legal Advisory and Secretary of the Board in Hispasat*



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