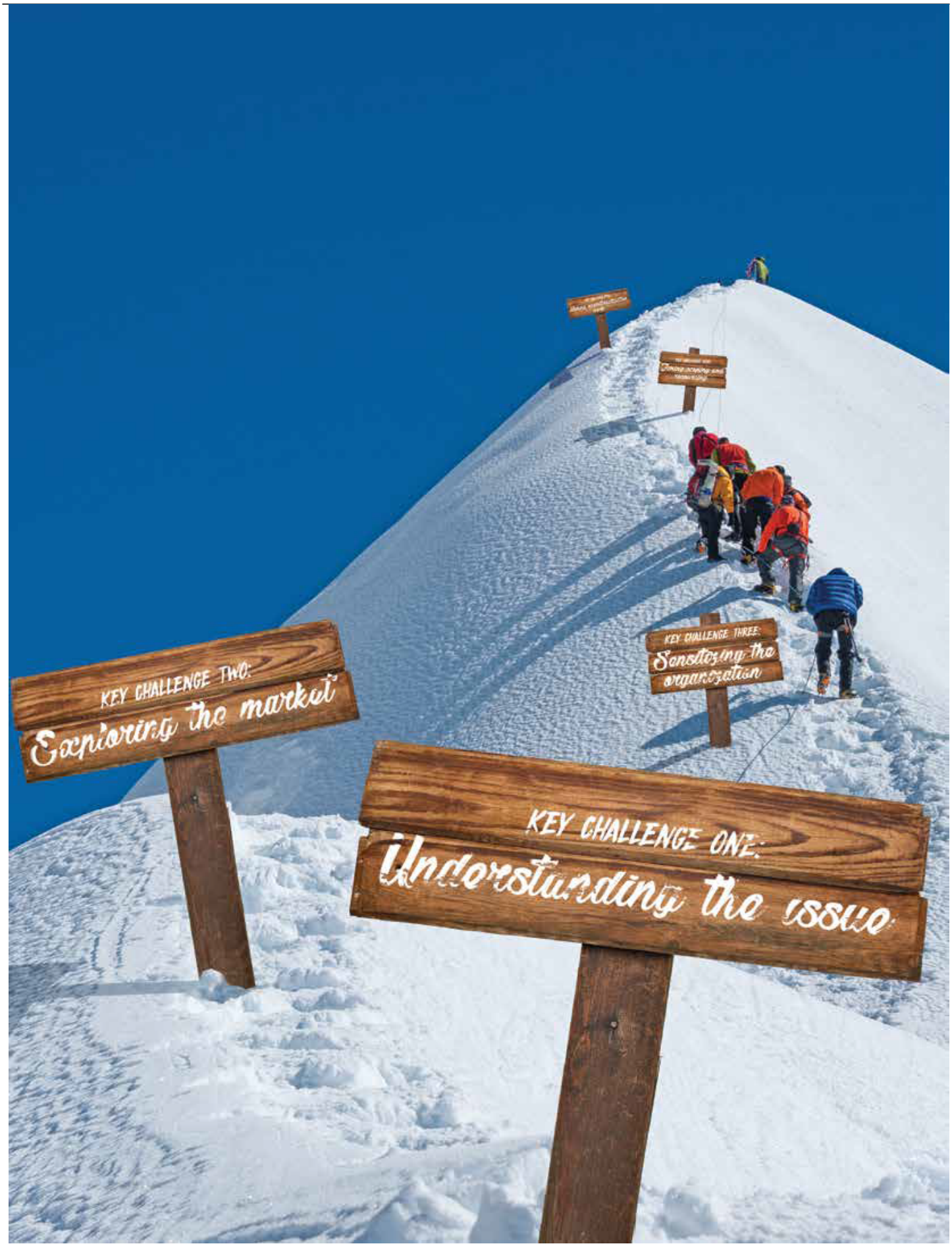
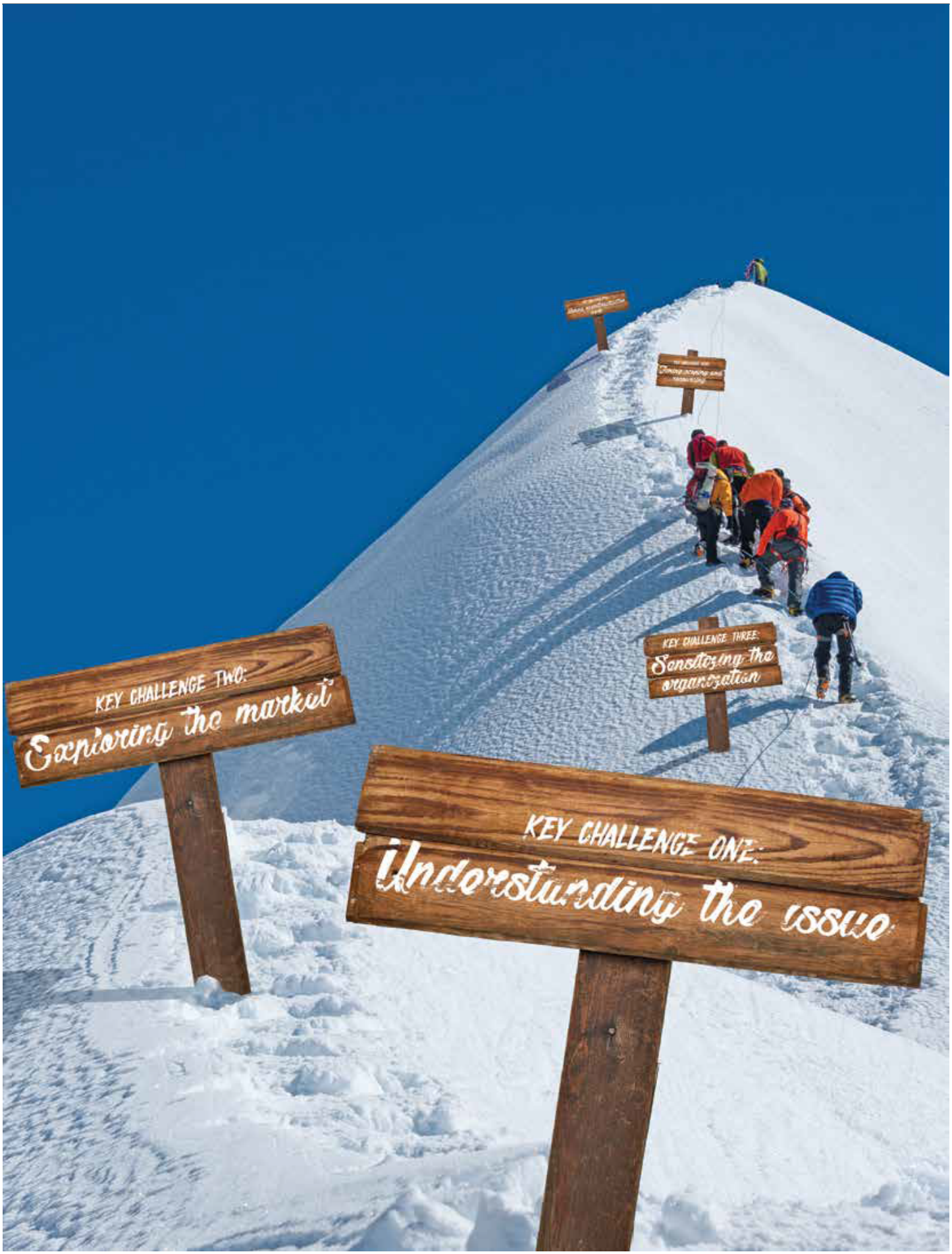
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How General Counsel Can Help the Company be Successful in its Data Journey

Technology, Privacy, and eCommerce


KEY CHALLENGE TWO:
Exploring the market
KEY CHALLENGE THREE:
Sensitizing the organization
KEY CHALLENGE ONE:
Understanding the issue


KEY CHALLENGE TWO:
Exploring the market
KEY CHALLENGE THREE:
Sensitizing the organization
KEY CHALLENGE ONE:
Understanding the issue

CHEAT SHEET

- ***Identify red flags.*** Companies often lack a sense of urgency in the area of data protection. Set up precautionary practices to ensure that company leadership understands the importance of this area.
- ***Follow the roadmap.*** A compliance roadmap should be created to guarantee that the company is prepared for any impending legislation.
- ***Enter the DPO.*** The General Data Protection Regulation requires the appointment of a qualified data protection officer (DPO) to help ensure that compliance measures are met. Support from the board and senior management is crucial for the DPO to succeed.
- ***Establish a culture.*** An effective data protection culture embeds data protection in the company, ensures that people at all levels deal with personal data responsibly, and outlines clear policies and internal communications.

As general counsel of a publicly traded company based in Europe, you work hard to strengthen your company's internal controls and compliance framework. Not a week goes by without receiving alarmist newsflashes about the European Union's impending General Data Protection Regulation (GDPR). These messages arrive immediately after you read the latest sensational news story about a peer company falling victim to a cyberattack. The board asks you to help design a compliance roadmap for privacy, outlining data protection and cybersecurity initiatives. You start investigating and encounter terms like opt-in, privacy by design, data breach protocol, the right to be forgotten, the cloud, big data, and the Internet of Things — on top of an impressive alphabet soup of acronyms like DPO, BCR, EuroPriSe, CSO, and PIA. You receive the newsletter of an activist shareholder highlighting cybersecurity as one of the key topics that will be discussed during the upcoming general shareholder meeting. The audit committee inquires as to whether the company should obtain cyber insurance. Your company's data journey has started in earnest. General counsel should play a valuable role during it. This article provides a practical perspective on the key challenges and suggested tactics to solve these problems.

The current technological revolution, fueled by tablet and smartphone technology, is taking innovation a step further than last decade's e-commerce platforms. Today's customer demands the ability to shop using a number of interconnected physical and virtual platforms, including tablets, smartphones, physical stores, and social media. Modern expectations require companies to communicate differently with their customers by offering a so-called OmniChannel customer journey. An OmniChannel customer journey permits the customer to move seamlessly between various shopping channels, including the physical store, web shop, and digital and social media. This is changing the face of retail. The traditional store concept is disappearing and morphing into experience shopping, complete with a coffee corner, online appointment booking, the absence of a physical cash register, payment by smartphone, virtual mirrors, and tech savvy sales staff equipped with tablets and smartphones.

This has sparked a data revolution that processes huge quantities of personal data. Initially, most customers or "data subjects" did not really mind sharing personal data on the internet and welcomed the subsequent pop-ups. A series of embarrassing data leaks have made the pendulum swing the other way. Now, customers are increasingly sensitive about the responsible use of their personal

data by businesses and by government. It has once again inspired lawmakers to try and bring legislation in line with the ongoing data revolution, including initiatives like the EU's GDPR and the ePrivacy Regulation.

This is where the general counsel comes in. General counsel operate best where business and legal intersect. The key message you will need to keep reinforcing is that protecting personal data is not a legal exercise. It is also not an IT thing. It is certainly not a "Check the Box" exercise. It is not a compliance project. It is not a project or even a series of projects. It is a company journey that will span many years. Neither legal nor IT can bring this journey to a successful completion. Data protection belongs to everyone. It is an integral part of the company's business model and a prerequisite for the company's long-term success. Customers are demanding the responsible use of their personal data. Companies that master this will secure a competitive edge visà-vis their competitors. Soon, there will be absolutely no room for data security slip-ups. Customers will disconnect from such companies and will loudly advertise their decision on social media.

Key challenge one: Understanding the issue

In-house lawyers tend to have some degree of comfort around insider trading, code of conduct, whistleblower procedure, and competition law. The past few years have seen many developments in these areas, particularly in the area of competition law. The area of privacy, data protection, and information security is not that new but it is not yet fully clear how to apply the updated rules in the wake of the ongoing technological innovation. In addition to understanding the legal issues, you also need to understand the technology. Spending time with your IT colleagues is time exceedingly well spent. Although in-house lawyers are generally not considered progressive techies by any stretch of the imagination, they do generally possess good analytical skills to help demystify, simplify, and operationalize a complex issue.

A good place to start is to understand the rights of the data subject — which can be summarized as the right to information, the right to correction or amendment, the right to objection, and the right to be forgotten or erased. An important case to know is the *Costeja* case. The *Costeja* case is the 2014 European Court of Justice's decision confirming the data subject's right to be forgotten by requiring internet search engines to consider requests from data subjects to remove links to freely accessible web pages resulting from a search on their name.

You also need to know the concepts of personal data and sensitive personal data. Personal data is all data relating to an identified or identifiable natural person or data subject. For instance, if the data is encrypted or hashed but is still identifiable, it is considered to be personal data. However, personal data that is anonymized according to applicable IT security standards no longer qualifies as personal data. Sensitive personal data is defined in a number of applicable data protection acts and includes medical data and the data of children. It is also important to know the principles for processing personal data. These include data economy, specific and legitimate purpose, transparency, accuracy, special protection for special or sensitive data, limited access, and security.

Key challenge two: Exploring the market

Once you have a working knowledge of the legal issues and the technology, you can start exploring the market. You should be prepared to face a multitude of advisors, offering a wide array of jargon, products, services, and price ranges. It seems that everyone holds a small piece of a very large puzzle. This makes the one-stop shop an elusive target. Businesses, advisors, and lawmakers

continue searching for a complete understanding of the right balance between the interests of businesses, government, and individuals. In the selection of your external advisors, you should not lose sight of the ultimate reality that the company will need to do most of the heavy lifting itself. It is the company that needs to establish a working data protection culture. You cannot outsource the project.

Key challenge three: Sensitizing the organization

Companies often lack a sense of urgency in the area of data protection. This is generally different from other compliance areas like competition law — where sensational news stories, including reputational damage, huge fines, and even imprisonment have caught the attention of the business executive community. Conversely, the GDPR allows for a fine of four percent of a company's global turnover. Many of the European Union's national data protection authorities have substantially increased their fines. The business community has not yet seen a high profile case where a company receives a huge fine, although there is a growing body of case law in addition to a seemingly endless series of cyberattacks.

The sense of urgency, however, will skyrocket in the event of a data crisis. A data crisis can occur in the form of a data protection authority investigation following customer complaints. It can occur from a data breach incident with the theft of the laptop from a senior executive. It can occur due to a case of so-called "social engineering," where a hacker assumes the virtual identity of the company CFO and instructs the finance department to make an important payment to a third party account.

How can general counsel increase the level of urgency of the business without having to go through a real data crisis? You can apply a number of tactics. You can share reports of data breach incidents in the market. You can refer executives to recent decisions like the Office for Civil Rights (OCR) of the US Department of Health and Human Services issuing a HIPAA civil money penalty of US$3.2 million to a company that issued unencrypted laptops and mobiles to its staff. You can organize a data breach exercise. You can work with internal audit and try and hack your web shop. You should also grasp every opportunity to speak at the company leadership forum or conferences on internal controls, compliance, and risk management to keep emphasizing the importance of this area for the company's continued success.

Key challenge four: Timing, scoping, and resourcing

Timing

A compliance roadmap needs to be drawn up, including important milestones like the start of the application of the GDPR on May 25, 2018. However, the roadmap should not come to an end on May 25, 2018, and your company's data journey is very likely to continue for many years after. Technological innovation is likely to continue, and the legal world will need to keep updating its legal framework and companies will need to keep updating its compliance framework.

Scoping: Data mapping and privacy assessment

An important first step in order to adequately address the scope of the work required is to establish a data map identifying all data and data flows in the business. This is a painstaking but crucial exercise. Do you know what data is processed by your company? Do you know where it flows? What personal data is processed? What data is processed centrally and locally? If data is transferred outside the

European Economic Area (EEA), you will need to look into EU model clauses, the end of safe harbor, and the emergence of the privacy shield. It is tempting to outsource this crucial first step, but the company is best placed to map its data flows.

As part of this exercise, you should also make a privacy assessment asking the following questions:

- Has management given attention to data protection and have you made it apparent that the privacy of individuals must be respected?
- Do you restrict the processing of personal data for the purpose(s) for which it is collected? Are the goals in line with the purpose for processing personal data?
- Do you make clear to the data subject how the personal data will be collected, including any passive data collection of which the data subject may not be aware? In other words, are you applying an opt-in policy?
- Do you check personal data for accuracy and completeness? Also consider that less and shorter is better. Apply data economy (no collection for future purposes and keeping of data which is no longer needed).
- Have you classified data into sensitive personal data, personal data, and non-personal data?
- Have you granted powers to employees so that only authorized employees have access to personal data?
- Do you apply sufficient security standards for storing and processing personal data?
- Have you implemented a data breach protocol?
- What do the operating companies do to protect sensitive personal data? Is the business diligent in the use of passwords and the regular resetting of passwords, privacy screens, secure printing, and authorizations for access?

Resourcing

In an ideal scenario, the company has a high sense of urgency, adequate budget, and a companywide network of dedicated DPO’s and Information Security Officers (ISO’s). It is an efficient and highly integrated organization where the business model and compliance policies are deployed consistently across the many jurisdictions where the company operates. In a more realistic scenario, there is some level of awareness without clear leadership. The work is loosely sprinkled over the legal, compliance, IT, internal audit, and finance departments — typically without a clear responsibility assignment matrix (e.g., RACI). Many organizations function largely as conglomerates of independently operating companies moving at different speeds.

This is an area where general counsel can bring their organizational qualities to bear. As the general counsel typically touches all areas of the business, he or she has a good feel for the company’s identity and can help tailor a charter, roadmap, and governance structure that works. Is the company EU centric or does it have a large geographic spread including developing economies? Is the company US headquartered? If so, is it transferring personal data to its sales offices oversees? Is the work force white collar or blue collar? Does the work force consist of engineers or sales people? Is the data centralized or decentralized? Is the company going through a big ERP overhaul or is it still relying on a number of legacy IT systems?

Key challenge five: Making operationalization work

Data vision

Although a lot of tactical work needs to be done, you should also spend adequate time defining the company's data vision. This will force you to make a number of important decisions. What data protection standard will you apply worldwide? Will you apply this standard consistently or will you be more lenient in developing economies? How are you factoring in Brexit? Will you be legalistic in your approach or practical? Is this a legal, compliance, IT, or business issue and who will be held accountable at the end of the day? The answer to the last question is crystal clear. Privacy, data protection, information protection, and cybersecurity are not legal, IT, or compliance tasks. Data protection belongs to everyone.

Policy and contractual framework

You should strive for a clear policy and contractual framework. This is also an area where general counsel can deploy his or her skills. You can write this as an all-inclusive policy or divide the issues in shorter approaches. You should at least cover data privacy, information protection and cybersecurity, data retention, social media, data breach protocol, and an IT end-user policy. Your policy localization philosophy is also an important success factor. Do you want the group policies rolled out in identical fashion across dozens of jurisdictions, or will you adopt a "freedom within a framework" approach allowing local color? The latter philosophy tends to be more effective. You should also make sure your third party agreements, notably with suppliers and franchisees, contain the required clauses on data protection. So often important third party agreements contain detailed provisions on price, service levels, and intellectual property — but barely provide for data protection and data transfer issues.

Data protection principles

A prerequisite for making policies alive in the business is to economize on legal and technological jargon and demystify the issue. One of the ways to do that is by building your compliance effort around a limited number of data protection principles. Such principles typically include data economy and accuracy, extra protection of sensitive personal data, limited access, and security.

Governance

An effective governance model includes a core team of legal, finance, internal audit, and IT supporting the DPO. The data protection community is led by the central DPO, who keeps the audit committee abreast of the progress in this area. This also requires an important reporting and measurement component. General counsel can play a valuable role in helping to develop a number of assessment and measurement tools to showcase the company's data journey progress to the board.

Data protection officer

Who wants to be the DPO? Anyone? The process of appointing a local and central DPO is a good test for the data awareness and data preparedness of the organization. The level of enthusiasm for this role is mostly low. Many companies do not necessarily have a full-time DPO. Often, this role is combined with other responsibilities. According to the GDPR and the Article 29 Working Party Guidelines, a DPO must be properly qualified and must have sufficient independence in the organization. They may not be in a position to determine the purposes or the means of the processing of personal data. As a rule of thumb, senior management positions are excluded. This is great guidance and makes sense from a separation of powers perspective. However, how will you

ensure the DPO will have sufficient weight in the organization to instill a data protection culture? Tone at the top and continuing support from the board and senior management are crucial to set the DPO up for success. Data protection officers are hard to find, but that should not prevent you from training your DPO on the important features of data protection law. Based on the outcome of the data mapping and privacy assessment, the DPO will need to design a DPO action plan — which will be the roadmap to reach compliance.

Data protection community

It is not enough to appoint a DPO and then leave the pulling and pushing to them. Data protection belongs to everyone. It is crucial to establish a true data protection community involving all stakeholders at the right moment. Once you have established that community, it is important to keep it alive. You can do this through continued education using live sessions, newsflashes, e-learning, and webinars. You should also use awareness campaigns with posters, hand-outs, and gadgets. Webinars are an excellent platform for sharing challenges and solutions with a large international audience. The DPO should realize they are not doing this alone and they should not keep reinventing the wheel.

Data protection culture

The Article 29 Working Party asserts that a DPO is required to promote a culture of data protection within an organization. This is excellent guidance, but is easier said than done. A data protection culture effectively embeds data protection in the company. It ensures that all people at all levels deal responsibly with personal data. Before you can achieve the goal of establishing a data protection culture, you typically require tone at the top and leadership commitment, clear policies and internal communications, effective training, measurement and reporting, responsible interventions, and accountability.

In order to accomplish this, you need to establish a behavioral change in the company. The above elements are stepping stones toward that change. All of your efforts will be useless if employees do not embrace the lofty goal of a data protection culture. This can happen when people do not understand the issue, are unable to digest the e-learning, and do not know what they should do differently. Your planned quantum leap in data protection should not detract you from the importance of baby steps. These baby steps are practical tips that explain what people can do differently every day. Making a number of small changes can make a big difference. These changes include requiring privacy screens for desktops and laptops, instilling password discipline, providing guidelines on data carriers (e.g., USB keys), and emphasizing the use of VPN and caution with using public networks, as well as encrypting all devices.

Job description: Data Protection Officer

Start: as quickly as possible.

Background: IT, legal, and compliance professional with experience working in an in-house environment. Preferably, all combined.

Required skills: Expertise in national and European data protection laws and practices, including an in-depth understanding of the GDPR, processing operations, information technologies and data security, the business sector and the organization, and the ability to promote a data protection culture

within the organization.

Responsibilities: Re-engineering the organization in order to ensure legally compliant processing of sensitive personal data, effectively preparing for application of GDPR. Information security knowledge is a plus.

DATA PROTECTION KEY PRINCIPLES

- Less is better;
- Legitimate and specific purpose;
- Transparency;
- Data economy and accuracy;
- Higher protection of sensitive personal data;
- Limited access; and,
- Security.

DAILY GUIDELINES

- Password discipline;
- Privacy screens;
- Caution with data carriers;
- Caution with public WiFi networks, use VPN; and,
- Only use encrypted devices.

Future

Irrespective of where companies are in their data journey, the end is not yet in sight. The ongoing technological innovation, with the lawmakers in hot pursuit, will stretch that journey over many years. An organization can never consider itself as having “arrived.” The world is digitalizing and also impacting companies’ vital legal processes, including digital signature and virtual annual general shareholder meetings. What if your virtual annual general meeting gets hacked? Privacy, data protection, and information security will for many years remain an area where general counsel and the in-house legal community can and should provide valuable support. General counsel can help demystify and operationalize a complex issue and help ensure the company’s continued success.

Data protection belongs to everyone. It is an integral part of the company’s business model and a prerequisite for the company’s long-term success.

Axel Viaene

Group General Counsel and Company Secretary

GrandVision