ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

How In-house Lawyers Enable Privacy and Data Protection

Technology, Privacy, and eCommerce

Arguably, one of the most significant challenges facing businesses the world over is privacy and data protection. Lawyers supporting businesses that grapple with this challenge need to be mindful of the fact that threats are ubiquitous, and we need to be prepared for the less obvious threats while simultaneously protecting against the known ones. A technical expert provided me with an analogy when we were discussing the different security measures that can be implemented and it resonates, he said, “If software is a house, it is important to ensure that the doors and windows are secure, but you always need to be able to detect if someone is coming through your roof or floor too.” This demonstrates the high stakes that data security teams face.

This challenge is significantly more complex for multinational companies that have to stay ahead of the curve on the ever-changing legal and regulatory framework across borders and seeing compliance in a way that works for the business. In addition to balancing complex legal and regulatory compliance, businesses must manage and respond rapidly to the constantly evolving threat profile of external security threats.

Managing this challenge from a legal perspective means in-house lawyers need to effectively partner with their technical and security teams, keep ahead of legal and regulatory developments, and provide solutions that allow for business efficacy.

Data security landscape

One of the most crucial teams, and areas of growth, in multi-national corporations is the security team. The emergence of new threat agents, coupled with the growth of existing threat agents commoditizing the activities, creates a dynamic requiring constant evolution in security measures, procedures, and goalposts. Through necessity, the data security of corporations must be ahead of the law when it comes to responding to the evolving risk vectors to ensure the safety of customer data, and not solely as a means for legal compliance.

Some prominent data security breaches have been generously unpacked by the companies that experienced them. They demonstrate the truth of data security requiring not only vigilance but agility and the means of detection must be constantly responding to the changing nature of attacks.

By partnering with the technical and security teams, in-house lawyers can understand the unique risks associated with the IT assets of the business, allowing lawyers to understand how best to support this security through policy and legal documentation. Additionally, lawyers can support their technical and security teams by ensuring they are aware of relevant legal and regulatory developments that affect the compliance framework relevant to the business. This is something we work to continuously improve at WiseTech Global. As the market and framework itself change, we need to ensure we are sufficiently agile to respond and also embed the principles in our strategy so we can future proof.

By partnering with the technical and security teams, in-house lawyers can understand the unique risks associated with the IT assets of the business, allowing lawyers to understand how best to support this security through policy and legal documentation. Additionally, lawyers can support their technical and security teams by ensuring they are aware of relevant legal and regulatory developments that affect the compliance framework relevant to the business. This is something we work to continuously improve at WiseTech Global. As the market and framework itself change, we need to ensure we are sufficiently agile to respond and also embed the principles in our strategy so we can future proof.

As a logistics software company with customers that include global logistics service providers, the global regulatory framework for privacy and data protection is at the forefront of our operations. We partner with our technical teams to ensure the principles that underpin the regulation are embedded operationally. In software development, our technical teams manage many factors from form and function of customer experiences to complexities involved with embedding customs law into operations. Therefore, early support from legal allows these teams to troubleshoot different build strategies, and ensures principles such as privacy by design are embedded without compromising any of the features that provide a good customer experience.

Customers need to know that their data is secure to discharge their own obligations to their customer base, while safeguarding what is a valuable commercial asset, and obtaining the advantage of the software they are using for operational benefit.

Legal and regulatory framework

Globally, there is a patchwork of different privacy and data protection laws and regulations that differ, sometimes conflict, and often overlap.

Although companies that do business in the European Union (EU) would be aware that the General Data Protection Regulation (GDPR) is one of the strictest, if not *the* strictest, data protection regimes globally, there continues to be local law nuance that adds additional layers of complexity, particularly

when it conflicts with the GDPR (i.e., certain domestic laws pertaining to discovery and litigation). Balancing the compliance with local law while ensuring that such compliance does not fall foul of the GDPR is not a simple task for any business. Therefore, understanding the laws and regulations in each jurisdiction is essential for in-house teams to manage this risk.

Balancing the current legal and regulatory framework in light of the recent reforms under way, along with those proposed, is a very fraught task for in-house lawyers. The privacy and data protection scope of legal compliance is burgeoning. Between the emerging enforcement action in the European Union, the situation with Brexit, and the proposed reforms in Australia and India, in-house teams need to remain abreast of these emerging challenges.

In the European Union, we are awaiting the new Standard Contractual Clauses, which are expected this quarter and will likely impact on agreements on foot for companies worldwide that conduct business in the European Union. We have yet to see the full implications of Brexit for the United Kingdom; although currently in a grace period, it remains to be seen what the new UK legislation will look like and if and when the European Commission will issue an adequacy decision for the United Kingdom.

There are reforms proposed for Australia's privacy law with specific intentions regarding user data protection; however, this has been delayed by recent world events. Proposed data protection legislation yet to be passed in India is intended to align with the GDPR concerning personal data, but goes further in respect of non-personal data. This will be an interesting reform to watch to see whether there is true alignment. The California Consumer Privacy Act (CCPA) also has the most robust data privacy law in the United States, adding complexity for any company doing business across the United States.

By understanding the in-force obligations and examining the proposed reforms and anticipating emerging trends, lawyers can support business agility. Additionally, by staying on top of these trends, in-house teams can help predict where laws are moving and start preparing their businesses for future compliance needs regarding privacy and data protection. An example of this would be to look to the most robust obligation and embed compliance with this into the operations of the company as a means of "best practice."

This provides operational benefit, particularly where there is global reach for an company because having to silo operations reduces operational efficiency. By examining the trends, lawyers can support best practice benchmarking across the company and provide sound legal rationale and a business case for efficiency. This consistency of approach means it is easier to initiate and repeat, which is more efficient and certain for global companies compared to disparate approaches.

Maintaining compliance with the most robust law provides a seamless way in which a business can continually improve, and lawyers can also be more efficient in their advice to the business. However, the most valuable gain from this strategy is operational gains. Technical teams will not need to rewrite code time and time again to respond to changes across geographies or implement certain security features for some locations but not others. This best practice strategy will also prevent remediation steps needing to be taken down the track once certain jurisdictions 'catch up' to other data privacy regimes.

Our role

The nature and role of the in-house lawyers in responding to privacy and data protection complexities

has changed over time. With the increase of cross border data flows, our understanding of data and our role in ensuring its protection has become more important. Although there are hefty sanctions across different locations that provide compliance incentives, this is not the only reason for compliance. Ultimately, we are all part of the data economy and, by holding ourselves and our companies to the high standards the market expects, we contribute to the integrity of the data economy.

We are not here to simply document the corporate compliance in contracts and policies, which, although important, does not demonstrate the significant value a lawyer holds in business partnering — providing knowledge to the business and providing solutions.

Knowledge

Keeping abreast of amendments to legislation and regulation is a pivotal part of in-house lawyers' value. With this knowledge, lawyers can advise businesses on live issues. There is also value in lawyers following developments of not only additional laws and regulations and reforms to same, but also trends in litigation and enforcement. Understanding how issues and responses to these issues are viewed by regulators and courts is essential for providing sound advice and recommendations that have been rigorously tested.

We also need to maintain our fingers to the pulse of market trends and what this means for global operations. It's a hefty task but one that makes in-house lawyers valuable.

The emergence of GDPR as a global framework rather than an additional compliance measure is a great example. An in-house lawyer watching this would have anticipated the current global reforms and set GDPR as the best practice benchmark for the business they support and, in doing so, would have little to do with additional compliance because additional geographies align their laws and regulations with GDPR. They can now efficiently respond to any adjustments to the most robust law or regulation and roll these out across all geographies of operation.

Partnering and solutions

By partnering with our technical and security teams, we embed privacy principles into the measures taken to keep data secure and to the design that the infrastructure data is housed in and transferred through.

Legal and technical partnering allows for an exchange of knowledge and influence that advances the partnership, understanding, and business operational efficiency beyond risk mitigation in contracts and other externally facing legal documentation. Therefore, there is widespread take-up of the principles that led to the enactment of the law and, where principles like this are embedded, compliance follows with ease.

In partnering with the business, lawyers are being afforded enhanced opportunities to provide solutions that support business strategy and efficiency, creating downstream opportunities for in-house legal teams to reduce reactionary issues.

Summary

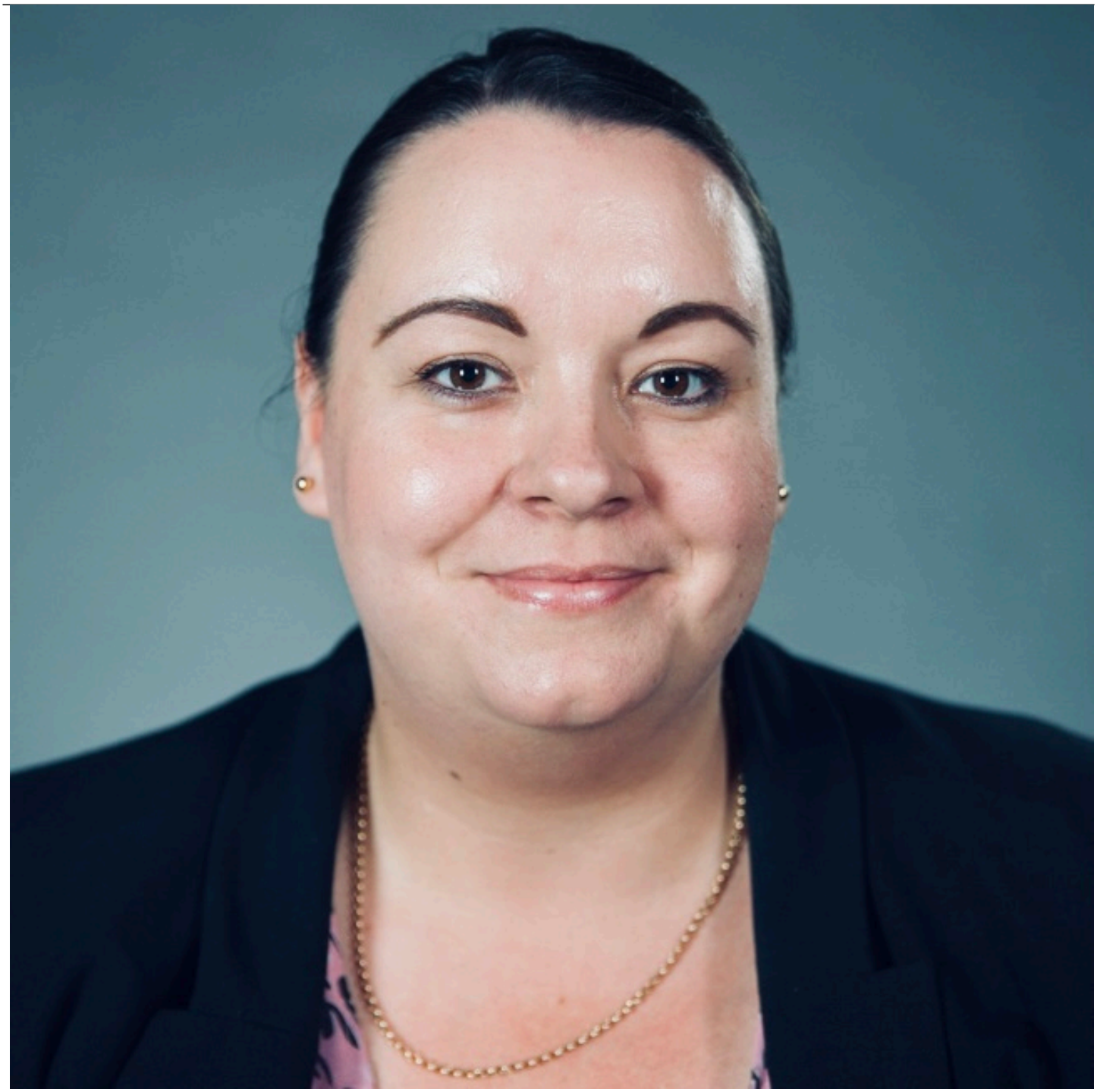
In-house lawyers play a crucial role in privacy and data protection, particularly in partnering with

technical and security teams to boost effectiveness in upstream processes that protect data and implementing protection against data breaches that are becoming more prevalent with the emerging and expanding external threat agents. By partnering with the business, embedding principles into the process and infrastructure, and maintaining an efficient best practice model, in-house lawyers can effectively mitigate the numerous risks associated with a disjointed international legal and regulatory framework.

Practical Tips

- Check-in with your security team to engage with them and understand current protected risk vectors and implemented measures.
- Understand any technical projects in the pipeline and find ways to support strategy and embed protections.
- Conduct regular training on privacy and data protection so all staff, company wide, understand their role in supporting the overall compliance strategy.
- Periodically review and update any internal and external policies to ensure they keep step with the prevailing law and regulation together with market conditions.
- Check your internal data transfer documentation for all group entities (if multi-national) and the extent of any EU overlap to ensure it contains the relevant (and updated) references to any Model Clauses and effectively enunciates the nature and purpose of any processing for each entity within the group.
- Check your suppliers, particularly any software suppliers that have operations outside the European Union, and ensure their privacy and data protection compliance is sufficiently robust (particularly because the privacy shield is no longer a valid mechanism).
- Keep watch for the upcoming release of the final Standard Contractual Clauses from the European Commission. It is expected, upon coming into force, that companies will have a limited window to adopt them into their relevant agreements.

Natalie Cromb



In-house Lawyer

WiseTech Global

As an in-house lawyer at WiseTech Global, Natalie works across the global business on a range of commercial matters. There she applies her specific interest in privacy and data protection, partnering with the business to provide proactive and innovative advice.