REPRINT

CD corporate disputes

THE CULTURE CLUB: DEVELOPING A PRIVACY CULTURE THROUGH EFFECTIVE TRAINING AND AWARENESS

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
APR-JUN 2020 ISSUE

www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

FTI CONSULTING™

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

EXPERT FORUM

THE CULTURE CLUB: DEVELOPING A PRIVACY CULTURE THROUGH EFFECTIVE TRAINING AND AWARENESS

PANEL EXPERTS

Vivien Lantree
Senior Privacy Lawyer
BT
T: +44 (0)7918 709 777
E: vivien.lantree@bt.com

Vivien Lantree is a principal privacy lawyer at BT. She is experienced in advising on global privacy programmes and opportunities to do more with data, be it in marketing, efficiency analytics and sharing for monetary value. She is always keen to find new ways of using data to extract the maximum value in a secure and ethical way.

Nina Bryant
Senior Director
FTI
T: +44 (0)20 3727 1124
E: nina.bryant@fticonsulting.com

Nina Bryant is an expert and thought leader in information lifecycle governance and privacy. She is experienced at leading global programmes to assess compliance with legal and regulatory requirements and developing and implementing solutions to reduce risk, drive cultural change and exploit the value from data and information.

Camilla Westlake
Director
FTI
T: +44 (0)20 3319 5727
E: camilla.westlake@fticonsulting.com

Camilla Westlake is a director in FTI's People & Change practice and has led internal communications initiatives and learning and organisational development solutions for global and UK-based clients in a range of sectors, including industrials, financial, telecoms, consulting, pharmaceutical, retail and manufacturing. She has also managed complex global projects for multiple international organisations, including campaigns around ethics and compliance, intellectual property and data protection. Key areas of expertise include change management, stakeholder mapping and impact analysis, organisational network mapping, strategic communications, leadership enablement and development, leadership comms, pre/post M&A planning and integration, and people and communications analytics.

CD: Could you outline some of the key challenges that commonly arise when implementing a global privacy programme?

Lantree: Finding common ground on a global stage can be very difficult. With standards for key issues such as data access and retention periods, among others, varying from region-to-region, it is often unclear where to set the bar. Communication across multiple languages and cultural nuances is another common challenge. Interpretation of values, words and systems will differ widely in each country. Even the best translation tools can still lead to nuances in meaning being 'lost in translation'. Teams need to be prepared for this, and work with key stakeholders and experts with knowledge about the unique aspects of each jurisdiction in order to determine a common threshold and communications strategy that makes sense companywide.

Westlake: With most people now owning a smartphone, as well as multiple other devices such as tablets, laptops and smartwatches, the average person is now much more aware of the risk of privacy breaches than ever before. A global privacy programme must not only cover local and international regulations, but also public opinion to provide investors, customers and employees with the confidence that their data, privacy and online security is secure. With increasing scrutiny into data protection, information security teams need to engage their employees to ensure they understand the risks of data leaks, as well as how to prevent them. Employee negligence is one of the top data risk factors for most organisations and they are a common entry point in data breaches. Investment and prevention measures are only effective if employees are informed, vigilant and understand their responsibility in protecting data in their organisations.

Bryant: One of the biggest current challenges is the complexity of the privacy legislation landscape. Countries around the world and individual US states all have unique and evolving laws and creating a global baseline framework that establishes compliance across all jurisdictions is extremely difficult. One way is to define an overarching global policy based on key principles, and then help build in the necessary exceptions and jurisdictional variations at a local procedural level. Additional challenges include varying jurisdictional expectations around how data should and may be used, which can often clash with objectives for leveraging big data. Key to any global privacy programme is balancing meeting a company's strategic objectives for data exploitation or insights, with securing data and protecting individual rights. Privacy programmes need to be an enabler to achieving strategic growth while ensuring appropriate security measures such

as encryption or anonymisation are embedded by design and understood by developers and architects. Another challenge can be scaling the programme to align with the size of the organisation's presence in different regions. For example, not every location will be large enough to support the roles and responsibilities of the global programme, and thus processes may need to be adjusted to fit with the local culture and organisational structure.

CD: Based on your experience, what factors do companies need to consider when developing a communications strategy?

Westlake: A communications strategy must always be rooted in what the business is trying to achieve. A great strategy helps employees understand what is needed of them, and then equips and inspires them to take the desired action. Data as a topic can seem dry, however privacy will resonate personally and is highly relevant. Companies must employ interactive and engaging communications campaigns around the topic of data protection, and these must be supported by reminding employees that by having a robust means of protecting privacy and data, a company is ultimately stronger, better and more fit for the future. The communications strategy is often further strengthened by highlighting how employees are essential partners in making this a reality. Engaging campaigns can be built around topics like safety, resilience and vigilance, all of which reflect the urgency and importance of this topic and are also themes that will be readily understood by employees as important.

> **"Investment and prevention measures are only effective if employees are informed, vigilant and understand their responsibility in protecting data in their organisations."**
>
> *Camilla Westlake, FTI*

Bryant: First and foremost, the communications strategy must bear in mind the organisation's culture, values and attitude toward change, as well as other major change initiatives already underway. Organisations that are undergoing rapid digital transformation may find it more difficult for the privacy voice to be heard above the noise. In these situations, combining privacy with existing programmes of work can be effective. Combining the privacy-related communications with overarching outreach around corporate strategy can help

relate the value of the privacy programme across the organisation and connect to wider strategic objectives which may have more resonance. In any communications strategy, proactively answering questions such as "why should I do things differently?" and "what is in it for me?" will help individuals understand the benefits of change, and their important role in adopting new policies and making the theory of privacy a reality in daily activities. If you cannot clearly and easily answer these questions you may need to rethink your core objectives and messaging. Organisations that fail to address these questions in their communications may find it challenging to get wider buy-in across the organisation and lose interest and momentum as a result.

Lantree: Building a privacy culture and a collaborative atmosphere should be the first step. Companies should talk to employees, take them along on the journey and make it real to them. This will help secure the critical buy-in needed to successfully implement a global privacy programme. Communication is key, and strategies should be built with the intention of creating a sense of unity. Teams should start early, keep people informed on the company's progress and set realistic expectations for the timeline. Companies should be clear on what is expected of individuals, and the role they play in contributing to the programme's success.

"Team meetings, annual events and long-term, themed campaigns are all viable approaches to getting the topic of privacy on the agenda, companywide."

Nina Bryant, FTI

CD: In what ways does a company's organisational culture impact its approach to communications?

Lantree: If a company is organised in a 'centre-out' way, this structure will be reflected in its communications style. While this may work for certain environments, at the global level, it can cause employees in disparate regions to feel isolated from the centre or the programme being introduced. Getting out in front of this proactively and designing communications that include and speak to each different location, will go a long way.

Bryant: Aligning with culture can make or break the success of a privacy communications initiative. Understand how the organisation sees itself – entrepreneurial, conservative, command and control, dispersed, tech-driven or traditional – and use mediums that fit that culture. A progressive, innovative company may benefit from digital communications mediums like internal social media channels and podcasts, while employees at a traditional company are more likely to respond to leaflets, desk literature or a face-to-face cascade of information at town hall events or team meetings. Culture will also inform what will generate enthusiasm from the start. Team meetings, annual events and long-term, themed campaigns are all viable approaches to getting the topic of privacy on the agenda, companywide. Creating a tie-in to strategic objectives and values is also effective. For example, a message of caring for data as a way to protect customers will resonate with employees at a healthcare company that is focused on patient care. But at an entrepreneurial tech start-up, it may be more appropriate to focus on the power of data and ensuring this is both protected and used to grow the business safely and compliantly.

Westlake: The culture of an organisation always plays an important role in how a communications campaign will be received. On the topic of privacy, it is critical that companies can determine if people are being asked to do things that run counter to the current culture. If so, the company is not just embarking on a communications campaign, it is embarking on a culture change which requires careful consideration. For example, if people are used to sharing information widely, then asking for a more conservative approach to data sharing may require specific guidelines. Likewise, if an organisation is highly hierarchical and authoritative, and you are seeking to solicit more bottom-up feedback about privacy breaches, then new policies and structures may need to support this change. A communications strategy which considers the company's culture will enable people to effectively transition to a new way of working.

> **"Companies should talk to employees, take them along on the journey and make it real to them. This will help secure the critical buy-in needed to successfully implement a global privacy programme."**
>
> *Vivien Lantree, BT*

CD: What steps should companies take to develop an effective awareness campaign?

Bryant: First, recognise the difference between awareness and training. Both elements should be embedded in the approach, but they are quite different. Awareness is about defining best practices and guidelines and providing visible and consistent reminders about what constitutes appropriate behaviour. Training is more involved and interactive, to teach employees about how to implement and follow the guidelines, and may be mandatory or regularly repeated, or available at point of need, such as being given access to a new application. An effective awareness campaign will help align all aspects of your programme – from policy and process updates to best practice and guidelines and how to access training. As such, it is important to have a clear connecting thread between all of these aspects. This could be a simple logo, a sophisticated campaign-based approach or something as simple as a strapline. Employees must understand the links between IT and information security – such as clean desk policies, password management and email security precautions, with responsibility to protect personal data and use or access it appropriately. Ultimately, awareness campaigns should help make the key messages around privacy and information security real and relatable in the context of day to day business activities.

Westlake: The most important aspect of driving awareness is recognising that awareness alone is not enough. Awareness building is critical to enabling employees to understand what is required, but to foster significant change or new behaviours, awareness must be followed up with more sophisticated enablement activities to provide employees with the capabilities and confidence to operate in a different way. In terms of steps for building awareness, a critical starting point is understanding what the overall objectives are – what do you want people to know and do differently? As with all communications, at each stage there is lively engaging, creative and visually engaging messaging and experiences to get employees on board with what you are aiming to achieve.

Lantree: What are the objectives of the campaign? What factors and benchmarks justify its success? What are the potential pitfalls? Companies must thoroughly consider these questions at the outset and build the campaign accordingly. This will guide positioning and help the team allocate the proper resources to ensure a successful communications push. The cultural background and interpretation of the reader will also apply. Take time to evaluate which messages may be misunderstood or what is at risk of being miscommunicated. Simplify as much as possible to avoid interpretation mishaps. Companies must work with local human resources (HR) departments and works councils.

Running training or awareness programmes past them can ensure that companies take cultural considerations into account.

CD: What training methods do you consider to be among the most effective?

Westlake: The best training approach is dependent on what the desired outcomes are, who the target audience is, and what you want them to know and do differently. Optimal trainings for building awareness include, but are not limited to, online webinars, presentations from leaders or experts and information-based materials, such as brochures. Developing skills or instilling a behaviour change requires a more sophisticated training approach. Some of the more effective methods tend to include face-to-face time, whether that is in a classroom or in a more informal setting, such as a lunch and learn. A live, in-person format provides employees with an environment where they can listen, learn and put into practice the knowledge and skills that are required of them; often in a 'test' environment where they can practice real situations. An integrated, multi-element training approach is often utilised for maximum impact.

Lantree: Interactive training is often the most effective means of employee education. Conference calls, video sessions, pre-recorded computer-based training and face-to-face meetings can all be leveraged, but they must be interactive, dynamic and engaging. Without an interactive training programme, organisations will struggle to generate engagement, test participant knowledge and evaluate the efficacy of the curriculum. Also, companies must avoid information overload. Outlining key takeaways, in a simplified and relatable way, is essential. Tools

like visuals and anecdotes can help ensure the information is digestible and memorable. Tying training to core principles or messages in new or existing policies, guidance and practices can reinforce those messages, and for remote working staff, particularly those who may not always have access to laptops due to the nature of their work or those who work as short-term contractors, consider training which is accessible by apps or mobile devices.

Bryant: As a rule, we need to make it easy for people to do the right thing – be that setting strong passwords or checking before they reply all to an email attaching a spreadsheet with large volumes of personal data. To achieve this, training should be engaging and demonstrate straightforward ways to incorporate best practices easily in daily activities. In-depth training at the point of need will typically drive the best results, such as lunch and learns or interactive 'train the trainer' sessions that provide face-to-face engagement. But these methods are intensive and can be impractical and costly to implement on a global scale, so in many instances, companies fall back on e-learning methods. While this enables an auditable approach to ensuring mandatory training is completed, it may not be the most effective method to deliver key messages. It also needs to be regularly refreshed and maintained. It is therefore helpful to have multiple training channels in addition to online training, such as presentations or videos which can be used at team meetings or watched at point of need, podcasts available to download, videos and key messaging at corporate events or town halls, and leaflets or tutorials to provide additional training messages. Whatever the medium, try to keep training business focused on real questions and problems, rather than too dry or theoretical.

CD: Could you explain how training and awareness help to reduce organisational risk?

Bryant: Strong training and awareness on key regulatory requirements, such as privacy and data protection, makes good business sense. It reduces the risk of non-compliance and demonstrates to clients and regulators that protecting personal data is a priority for your organisation. How organisations protect and use their customers' data is now a key element of their brand and reputation and any perceived inconsistencies or breaches can do significant market damage. Some privacy regulations, including the GDPR, require training and awareness to enable full compliance. Under laws with these types of guidelines, failure to embed a culture of privacy into the organisation may be interpreted as a lack of compliance and could influence the severity of a penalty in the event of an enforcement action. Sound training and awareness programmes also reduce the risk of an accidental data breach. When

employees are aware of the issues and trained on best practices, they are less likely to fall foul of the policies, and more likely to escalate mistakes. This strengthens incident response and therefore reduces the overall risk of exposure. A global privacy framework with awareness and training at its heart helps future-proof the organisation against new and evolving legislation. When an organisation is ahead of the curve and has developed a culture of privacy and security, it is bolstered to weather ongoing global legislative change and can adapt to maximise data as a strategic asset, while enabling compliant data handling practices.

Lantree: Training and awareness informs employees, contractors, suppliers and customers of the risks associated with data processing and usage. It unites them to their unique and important role in protecting sensitive data. It empowers them with tools to help mitigate risks and add value to the organisation. These are essential to ensuring everyone plays their part. When a privacy compliance culture is nurtured and operated at a global scale, the organisation is rewarded with a strong foundation for reducing myriad risks.

Westlake: When it comes to privacy and data protection within an organisation, there are multiple layers of risk to be cognisant of. By being aware of the potential challenges and the impact of exposing secure data, employees will be better placed to operate in a way that ultimately protects the business and its key stakeholders. Awareness building and training should work alongside each other as they are both equally as important for informing and enabling employees. An integrated communications, engagement and training strategy will ensure that all employees know what they need to do, how they need to do it and why it is so important. It can also highlight what may occur if the appropriate policies and process are not adhered to. A workforce that it is equipped to manage and store private information will reduce the extent to which an organisation is at risk of data exposure or regulation breaches. CD