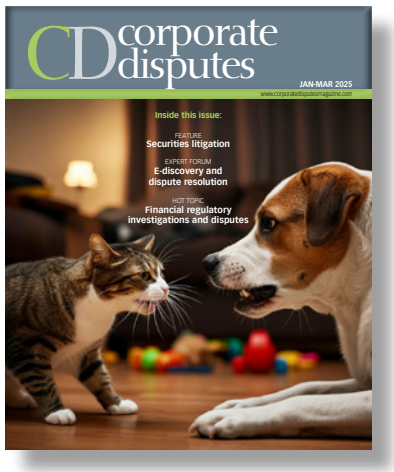
REPRINT

DATA PRIVACY AND CYBER SECURITY DISPUTES

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JAN-MAR 2025 ISSUE



www.corporatedisputesmagazine.com

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

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

MINI-ROUNDTABLE

DATA PRIVACY AND CYBER SECURITY DISPUTES

PANEL EXPERTS

Taryn Kilkenny Crane
Practice Leader
BDO
T: +1 (301) 354 2583
E: tcrane@bdo.com

Taryn Kilkenny Crane is the privacy and data protection practice leader at BDO. She has a focus in privacy, data protection and privacy technology services, and has consulting experience working across several markets including hospitality, retail, financial services, insurance, technology, life science, industrial and nonprofits. She also has experience advising and delivering privacy programme solutions, ranging from maturity assessments, programme development and technology implementation.

Ahmed Baladi
Partner
Gibson, Dunn & Crutcher LLP
T: +33 (0) 1 5643 1300
E: abaladi@gibsondunn.com

Ahmed Baladi is a partner in the Paris office of Gibson, Dunn & Crutcher LLP and co-chair of the firm's privacy, cyber security and data innovation practice group. He specialises in information technology and digital transactions, outsourcing, data privacy and cyber security. He has developed considerable experience in a wide range of technology and digital matters. His practice covers complex technology transactions and outsourcing projects, particularly in the financial institutions sector.

CD: Could you provide an overview of the critical risks for companies arising in connection with data privacy and protection? To what extent can weaknesses in cyber security lead to disputes?

Crane: The looming threat of data breaches and ransomware attacks remains a significant risk for companies, stemming from hacking, insider threats or inadequate security measures. The repercussions extend far beyond initial investigation and remediation. After notifying regulators and affected individuals, companies often face a prolonged period of costly litigation, class actions, negotiations and ongoing monitoring. Aside from data incidents, regulatory investigations and enforcement pose another substantial risk. With regulators allocating more resources to probe complaints and conduct independent investigations, organisations found non-compliant face severe consequences. These investigations often arise from insufficient security controls or the excessive use and disclosure of personal data. The financial and reputational damage from these risks can be devastating, underscoring the need for robust cyber security measures and strict adherence to data protection regulations.

Baladi: Since the General Data Protection Regulation (GDPR) entered into force in 2018, data protection authorities have become increasingly active in enforcing it across the European Union (EU). As a reminder, non-compliance with GDPR obligations can result in fines being imposed on companies – up to 4 percent of their worldwide turnover. However, national authorities that impose these fines can also decide to make the decisions public, in which case it is likely that the penalty will have large media coverage which could affect the company's reputation. On the cyber security front, companies can be fined under the GDPR for failure to ensure the security of the personal data processed by implementing adequate security measures. It should be kept in mind that other regulations that are cyber security-specific, such as the Security of Network & Information Systems Regulations and the Cyber Resilience Act, will impose additional obligations for certain actors in relation to cyber security, as well as fines. In addition, failure to implement adequate security measures can lead to disputes with affected business customers or even consumers over responsibility and compensation issues in relation to loss or destruction of data.

CD: Are you seeing any common types of data privacy disputes? Do recent cases highlight any recurring themes of note?

Baladi: In the EU, the legal framework for privacy litigation allows for individual lawsuits and for class actions. Under the GDPR, individuals who suffered damage as a result of a GDPR infringement have the right to receive compensation and the EU Representative Actions Directive harmonises the procedures for class actions in all member states as some were still lacking specific mechanisms. To date, the number of privacy disputes are limited in the EU, unlike in the US where they are common practice. However, we note certain privacy disputes in particular in the Netherlands where a consumer rights group claimed that a company illegally tracks its users' online activity, or software companies were allegedly collecting and processing personal data of internet users for commercial purposes. In Germany, local courts are reportedly receiving many complaints from users as a result of a data breach. Therefore, we should expect more class actions to come in the EU in the near future.

Crane: A growing concern in regulatory enforcement and class actions is the sharing of personal data with third parties, especially through website and mobile app tracking technologies. Plaintiffs are increasingly citing wiretapping claims under the California Invasion of Privacy Act due to cookies, pixels and other tracking technologies shared with third-party vendors. Additionally, webform entries or search phrases embedded in URLs are often shared inadvertently with third parties, including advertisers, creating further legal pitfalls. The surge in these disputes highlights a clear demand from both regulators and individuals for greater transparency, controlled data sharing and respect for consent preferences. Companies must navigate these challenges carefully, ensuring robust data protection practices to maintain trust and compliance in an increasingly scrutinised digital landscape.

CD: In the event of suffering a cyber security breach, what initial action should an affected company take with regard to any data protection concerns?

Crane: After an organisation completes the initial incident response to identify and contain a breach, a thorough forensic investigation becomes crucial. Engaging a skilled third party to analyse, rationalise and de-duplicate data is essential to pinpoint affected individuals, their locations and the data elements involved. This precise information is vital for determining which jurisdictions require notification and adhering to their specific timelines. For example, the EU's GDPR mandates notification within 72 hours of a breach, which requires swift action to comply with regulatory deadlines. Post-notification, companies should brace for a surge in data subject requests, as individuals will seek

answers, express concerns, and request access to or deletion of their personal data. To manage this influx effectively, organisations must enhance their data subject request processes, ensuring they can respond promptly and accurately, thereby maintaining trust and compliance in a challenging environment.

Baladi: From an EU legal perspective, upon suffering a cyber security breach, affected companies should take a number of actions. First, assess whether any personal data was affected by the breach, which can include destruction, loss, alteration, unauthorised disclosure, access or any loss of confidentiality, availability or accuracy of the personal data processed. Second, assess whether the breach impacted individuals located in the EU to determine whether the GDPR is applicable. Third, assess their status in relation to the personal data – data controller or data processor – to determine their obligations in relation to the personal data breach. Fourth, when acting as a data controller, the company should notify the relevant data protection authority within 72 hours unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Fifth, when acting as a data processor, the company should notify the data controller without undue delay of the breach. Sixth, evaluate whether they should also notify data subjects of the breach, which is necessary if the breach is likely to result in a high risk to the rights and freedoms of natural persons. Finally, notify national security agencies if the organisation is considered an essential and important entity.

> **"Companies should conduct a comprehensive data mapping and data classification exercise, as well as identify their status as controller or processor in relation to the processing of personal data."**
>
> *Ahmed Baladi, Gibson, Dunn & Crutcher LLP*

CD: Could you highlight any recent, high-profile incidents which illustrate the data privacy risks impacting businesses worldwide? What lessons can be learned from how these disputes were addressed?

Baladi: High-profile incidents exposing millions of customers' personal data, including sensitive information, highlights companies' vulnerabilities

leading to consumer concerns and complaints, as well as regulatory investigations. Key lessons to draw from major incidents include the need to prioritise strong security measures and continuously invest in them to keep up to date, complying with regulatory requirements, responding swiftly to breaches, offering remediation measures, training staff and having an adapted cyber insurance policy. These actions are essential for mitigating the risks of data privacy disputes.

Crane: This year's most talked-about incident involves a ransomware attack on a major healthcare company. As custodians of vast amounts of personal and health data, this company and its parent organisation are prime targets for cyber criminals. While large healthcare and insurance entities are high-profile targets, these types of security threats can impact organisations of any size, severely disrupting operations and financial stability. Earlier this year, it was revealed that attackers infiltrated an employee's system using stolen credentials, exploiting the absence of multifactor authentication (MFA). Implementing MFA and similar controls is crucial to prevent unauthorised access. Despite paying the ransom, there is also no assurance that the stolen personal data has been deleted, leaving individuals' information at risk. This incident underscores the financial and reputational damage that can ensue, highlighting the urgent need for robust cyber security measures across all organisations to help avoid such incidents from the start.

CD: In a changing, challenging legal and regulatory landscape, how important is it for companies to have a data privacy compliance programme in place to address the impact of potential disputes? What are the key elements?

Crane: In today's ever-evolving regulatory landscape, a robust privacy compliance programme is essential for organisations to proactively mitigate risks and demonstrate adherence to applicable laws. Flexibility and adaptability are key, as regulations continue to change. In disputes, both regulators and plaintiffs will scrutinise the controls in place at the time of an incident to assess the programme's adequacy and potential negligence. Key components of a compliance programme include governance, data inventory, risk management, policies, training, data subject rights, third-party management and incident response. However, specific focus areas can significantly mitigate disputes. Effective data management and retention are crucial, as many incidents are exacerbated by excessive personal data that could have been purged or anonymised. A solid information security foundation, implementing best practices across systems, is also vital. Lastly,

a robust incident response plan ensures swift, compliant action during breaches or disputes, aligning with regulatory expectations and minimising impact.

Baladi: It is crucial that compliance programmes are kept up to date for businesses to manage personal data responsibly. Having a comprehensive data privacy programme helps mitigate risks by ensuring that a company is proactively addressing privacy concerns and protecting the personal data of its customers and employees. In this respect, a data privacy compliance programme should include several key elements. Companies should conduct a comprehensive data mapping and data classification exercise, as well as identify their status as controller or processor in relation to the processing of personal data. They should have policies and procedures in place to comply with applicable privacy obligations, including a process to assess what regulations apply, such as in Europe, the US and Asia-Pacific. They should also implement security measures appropriate to the level of risk associated with processing activities – taking into account the nature of the data processed and the purposes – as well as an incident response plan. It is also important to conduct regular privacy and security training for employees, as well as regularly assess the policies and measures in place to identify any vulnerabilities and update requirements.

CD: What essential advice would you offer to companies in terms of preparing for, and responding to, a cyber security incident that raises data privacy concerns which may result in disputes, including litigation?

Baladi: The best way to ensure that companies are best prepared for cyber incidents is for them to have robust security procedures in relation to data access, encryption, disaster recovery and incident response. Security measures should be updated to account for new threats and an incident response plan developed accordingly. It is also important for companies to conduct internal and external security audits and penetration tests to identify vulnerabilities and implement mitigating measures. Providing cyber security and privacy training to employees is also beneficial, as is a cyber insurance policy. When responding to cyber security incidents, it is highly recommended that companies are assisted by an external technical investigation team that will provide a detailed report containing at least information on the origin of the breach, the affected data and individuals, whether the threat is still active or if the incident can be considered closed, and appropriate remediation measures. This information will be necessary for notifying data supervisory authorities and data subjects where required.

Crane: First, companies should establish a robust incident response plan that clearly defines roles, responsibilities, key contacts and procedures. This plan should encompass steps for containment, remediation, recovery and communication, ensuring timely notification to all necessary parties. Engaging legal and compliance teams early is crucial to align the response with regulatory requirements and prepare for potential litigation. Additionally, companies should document every aspect of the incident meticulously, including the process, decisions made, actions taken and the rationale behind risk-based choices. This detailed record keeping is vital for legal defence and post-incident analysis. Lastly, companies should implement a transparent communication strategy to inform regulators and affected individuals. Clear, honest communication fosters trust and helps mitigate reputational damage. By proactively addressing these elements, companies can navigate cyber security incidents more effectively, safeguarding their reputation and maintaining stakeholder confidence.

CD: Looking ahead, what are your predictions for the data privacy and cyber security landscape? What factors are likely to shape future disputes?

Crane: As consumers become increasingly savvy about their data rights, they demand greater control and privacy, which will likely lead to a greater surge in class actions and litigation in jurisdictions that allow it. This shift should compel organisations to prioritise transparency and robust privacy practices. The rise of artificial intelligence (AI) and machine learning will also transform the cyber security landscape, enhancing defences while also being exploited by cyber criminals. Organisations must equip themselves with the necessary skills and technologies to proactively predict and mitigate these evolving threats. Additionally, the adoption of zero trust security models will continue, emphasising stringent identity verification and access controls. Companies must stay ahead by implementing these and other leading techniques, demonstrating

> **"Effective data management and retention are crucial, as many incidents are exacerbated by excessive personal data that could have been purged or anonymised."**
>
> *Taryn Kilkenny Crane, BDO*

their commitment to maintaining robust security measures. Embracing these changes is essential for organisations to build trust, ensure compliance, and safeguard their reputation in an increasingly complex privacy and cyber environment.

Baladi: The data privacy and cyber security landscape will continue to evolve and feature more advanced threats, in particular powered by generative AI tools. In this respect, ransomware targeting companies and enabled by phishing attacks will be more efficient as threat actors will be able to create the near-perfect illusion of legitimate emails via AI tools. This evolution points to the need for more caution, robust cyber security measures and defence strategies including advanced incident response plans, and for enhanced employee awareness and training. In addition, the regulatory landscape will evolve due to upcoming new cyber regulations imposing new obligations on a varied range of actors. For instance, the recently published EU AI Act imposes an obligation on high-risk AI systems to report serious incidents, and the recently adopted EU Cyber Resilience Act will obligate manufacturers of products with digital elements to disclose any exploited vulnerability contained in those products or any severe incidents which have an impact on product security. CD