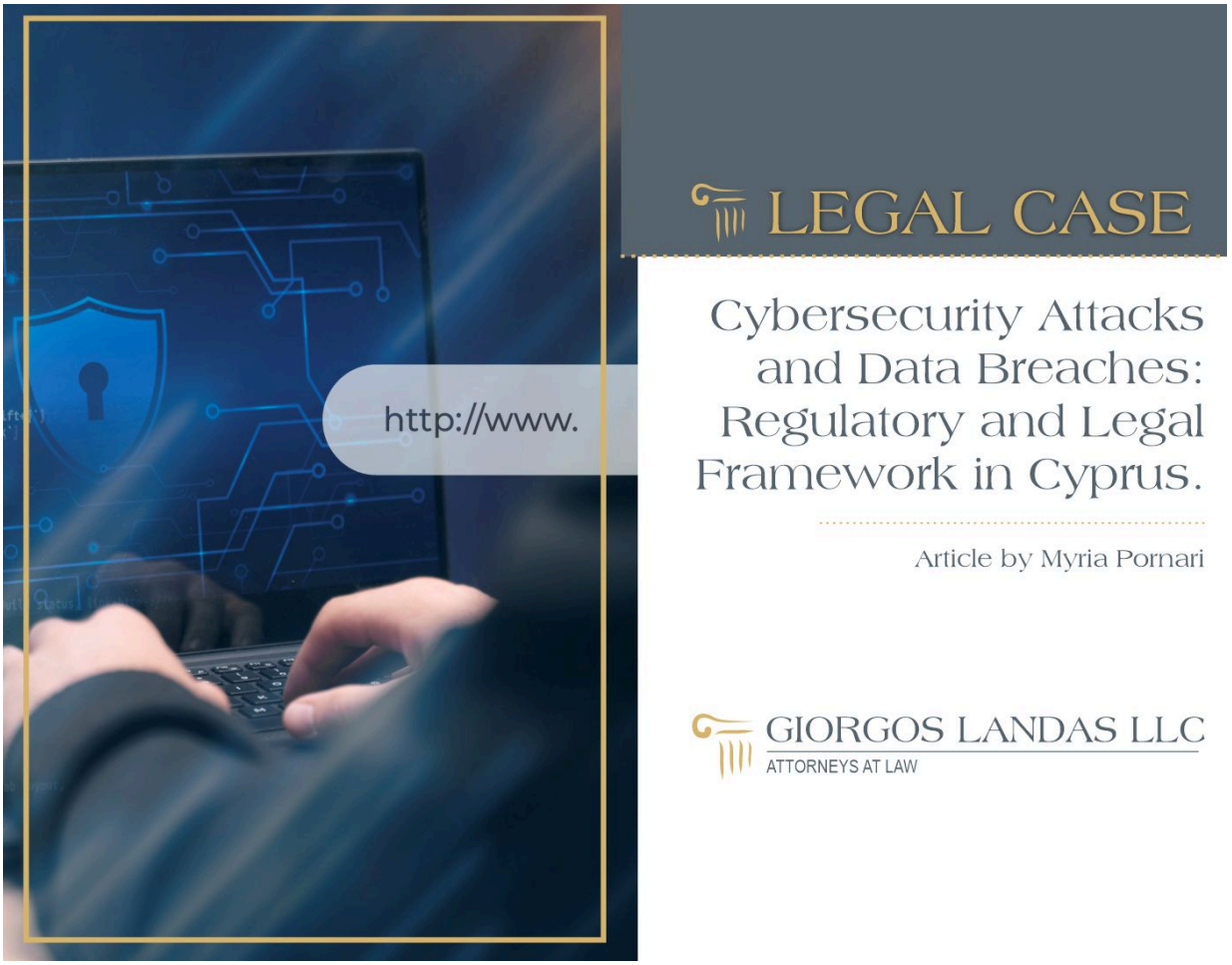
Cybersecurity Attacks and Data Breaches: Regulatory and Legal Framework in Cyprus.



By Myria Pornari, Associate at Giorgos Landas LLC

In the digital age, cybersecurity breaches—commonly referred to as "hacking incidents"—have become increasingly disruptive, posing significant legal, financial, and reputational risks to organizations. These incidents can lead to unauthorized access to sensitive information, causing harm not only to the affected companies but also to individuals whose data may be compromised. It is therefore imperative for Cypriot companies to be well-informed about their responsibilities and to take prompt action to mitigate the consequences of such breaches. This article provides a concise overview of the key guidelines that should be followed in the event of a data breach.

First and foremost, under the General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as "the Regulation") — organizations have clear legal obligations in the event of a personal data breach. Pursuant to Article 33 of the regulation, when a breach occurs, the Data Protection Officer (DPO), or another responsible person within the organization, must

notify the Office of the Commissioner for Personal Data Protection without undue delay and, where feasible, no later than 72 (seventy – two) hours after becoming aware of the breach. This timely notification is critical to ensure appropriate regulatory oversight and to protect the rights of data subjects.

It has to be noted that if such notification is not made within the 72-hour timeframe, the entity must provide a justified explanation for the delay. The notification must, inter alia, include the nature of the personal data breach, the categories and approximate number of data subjects affected, the likely consequences of the breach, and the measures taken or proposed to address the breach and mitigate its potential adverse effects. In reference to the above – mentioned according to article 34 of the regulation, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must also communicate the breach to the data subjects without undue delay, using clear and plain language to describe the nature of the breach.

Furthermore, the hacking incident must be reported to the relevant police authorities without undue delay. Timely notification is essential to enable law enforcement to initiate appropriate investigative and protective actions, mitigate any ongoing or future threats, facilitate potential criminal proceedings, and uphold the rights and interests of the individuals whose personal data may have been compromised.

While criminal prosecution is a vital aspect of addressing cybercrime, victims of such incidents may also seek civil remedies through the courts to obtain compensation and prevent further harm. In the aftermath of a cyber incident—such as hacking, data breaches, or unauthorized interference with servers—interim reliefs play a critical role in preserving evidence, protecting sensitive data, and preventing further harm. These remedies are granted by the court on an urgent and often ex parte (without notice) basis, particularly where the risk of irreparable damage or destruction of evidence exists. The most essential interim reliefs in such cases are inter alia the following:

1. Prohibitory Injuctions: A prohibitory injunction restrains a party—typically the alleged hacker or a third party in possession of compromised data—from engaging in harmful conduct. In the context of cyber incidents, such injunctions may prohibit the continued unauthorized access to systems or databases, distribution, sale, or publication of stolen data as well as the communication or disclosure of confidential or sensitive information. These orders are often accompanied by ancillary reliefs, including requirements to preserve digital records or log user activity.
2. Norwich Pharmacal orders: it is essential to state that Norwich Pharmacal Orders can be characterised as a very useful tool in such cases and are used to compel third parties (such as ISPs, hosting providers, or platforms) to disclose the identity of anonymous wrongdoers — for instance, the IP address or account information used in the hacking. Such orders are essential when the perpetrator's identity is unknown,

allowing the victim to gather necessary information to initiate formal proceedings. When hackers are unknown, claimants often rely on Norwich Pharmacal orders to compel disclosure from third parties to trace the culprit before pursuing full civil or criminal actions.

3. Mandatory Injuctions: Unlike prohibitory injunctions, mandatory injunctions compel a defendant to undertake specific actions. In cyber-related claims, courts may order the defendant to: Return or destroy unlawfully obtained data, disable accounts or services used to carry out the breach and Provide access credentials or assist in forensic investigations. Given their invasive nature, mandatory injunctions are generally granted only where the claimant can demonstrate an overwhelming need and the inadequacy of alternative remedies.
4. In reference to the above – nentioned, Gagging orders (or non-disclosure injunctions) may be granted to: Prevent the media or other third parties from reporting on the incident, prohibit the publication or further dissemination of compromised data and protect the identity of affected individuals or parties under investigation.
5. An Anton Piller order is a powerful civil court injunction that permits the claimant to enter the defendant's premises without prior warning to search for, inspect, and seize evidence relevant to the claim. In the context of hacking or illegal interference with computer systems, Anton Piller orders serve critical functions, including inter alia the following: Seizing compromised data or stolen information and preventing the destruction or concealment of digital evidence since hackers or perpetrators may delete files, erase logs, or otherwise tamper with electronic data once they learn of legal action.

It is essential to state that English case - law treats hacking incidents with increasing seriousness, recognizing them as significant violations of property rights and personal privacy under common law principles. Courts have consistently upheld that unauthorized access to computer systems constitutes a tortious wrong, often framed as trespass to chattels or misuse of private information. Additionally, English courts have demonstrated a strong willingness to grant robust interim remedies—such as injunctions and Anton Piller orders—to prevent ongoing harm and preserve crucial digital evidence. Through precedent, the judiciary emphasizes the need to protect both commercial interests and individual data privacy, balancing the rapid technological developments with established legal doctrines. This evolving body of case law reflects a proactive approach in addressing cybercrime within the civil justice system alongside parallel criminal prosecutions.

In conclusion, addressing hacking incidents requires swift action, clear legal obligations, and effective remedies to protect data and prevent further damage. Legal systems are evolving to respond firmly to cyber threats, balancing the need for security with individual rights. Coordinated regulatory, criminal, and civil measures are essential to combat and mitigate the impact of cybercrime in today's digital world.