Major Data Breaches – The Importance of Taking Care of Personal Data

AUTHOR / KEY CONTACT

Ruth Chornolutskyy
Associate

Ruth.chornolutskyy@la-law.com
01202 786188

Some recent major data protection breaches have demonstrated the need to take our responsibilities for protecting personal data very seriously. This includes, amongst many other things:

- properly educating staff in your organisation to minimise the likelihood of breaches arising due to human error; and
- having proper policies and procedures, both to demonstrate compliance with data protection legislation and to ensure an organisation functions as well as possible in the aftermath of a cyber-attack so as to try to minimise the negative consequences.

The recent cases below demonstrate how potentially catastrophic data breaches can be both due to human error and cyber-attacks.

Threat faced by the Police Service of Northern Ireland following release of highly sensitive information:

In response to a Freedom of Information request to the Police Service of Northern Ireland ("PSNI"), what should have been released was a table containing just a breakdown of the number of people holding positions such as constable in the PSNI. However, in error, the PSNI shared an Excel spreadsheet containing un-redacted information of over 10,000 police and civilian personnel, including the surname and first initial of every employee, their rank or grade, where they are based and the unit they work in (including sensitive areas such as surveillance and intelligence). It is understood that the details were then published online on the on "What Do They Know" website, before being removed a couple of hours later at the request of the PSNI when they became aware. The breach is currently being attributed to human error and has been described as a "breach of monumental proportions" and probably the worst data breach in the PSNI's 22-year history.

During almost 30 years of violence known as the Troubles in Northern Ireland, 302 police officers were killed and members of the PSNI have been targeted in gun and bomb attacks in the years following the Good Friday

Agreement. In 2022, the terrorism threat level was downgraded for the first time in 12 years but, in February this year, senior PSNI officer Det Ch Insp John Caldwell was seriously injured in a shooting in Omagh, County Tyrone and the terrorism threat level in Northern Ireland has gone back up from substantial to severe, meaning an attack is highly likely. The leak of such sensitive information is therefore potentially a great threat for police officers in Northern Ireland and their families.

The Police Federation has called for an urgent inquiry with its chairman saying, "Rigorous safeguards ought to have been in place to protect this valuable information which, if in the wrong hands, could do incalculable damage." and that it would have been a "potentially calamitous situation" had the spreadsheet contained the addresses of the officers, which fortunately it did not.

The Alliance Party leader said there would need to be a full and frank investigation into the circumstances of the breach, including why the data was available to be released in unencrypted form and expressed her concerns that the digital footprint would be almost impossible to eradicate.

Complex Cyber Attack on the UK's Electoral Registers:

The UK's elections watchdog has warned people to watch out for unauthorised use of their data, following access by hackers to copies of the electoral registers from August 2021. The information accessed is understood to contain names and addresses of people in the UK who registered to vote between 2014 and 2022, including those who opted to keep their details off the open register. It is also said to contain the names, but not the addresses, of overseas voters. Whilst the number of people affected is currently unknown, the register for each year contains the data of around 40 million people.

The attack was identified in October 2022, but has only now been made public, with the Electoral Commission saying it was necessary to first put a stop on the hacker's access to the system and security measures in place as well as try to establish the extent of the risk caused to individuals. It is understood though that attackers had first accessed the computers more than a year earlier, in August 2021 and experts have questioned how the attack went unnoticed for so long.

The seriousness of the attack for ordinary citizens has been downplayed on the basis that much of the information is already in the public domain, however there are concerns that the information held in the registers could be combined with other data in the public domain which could lead to profiling of individuals.

The Electoral Commission has said it does not know who is responsible for the attack, and that no groups or individuals have so far claimed responsibility, however, it has taken steps to secure its systems against future attacks, including updating its login requirements, alert system and firewall policies. The breach is being investigated by the Information Commissioner's Office.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

Conclusion:

These stories demonstrate that data protection is a very serious subject for all organisations, whether in the private sector or the public sector. The consequences of a data protection breach can be catastrophic for both the individuals whose data is affected and the business itself.

The Information Commissioner's Office has extensive powers to take public and punitive action against organisations which fail to adequately protect the personal data they process. This can be very damaging for a business from both a financial and reputation perspective.

Many security breaches come down to human error so educating staff in your organisation on their data protection obligations is paramount to minimise the likelihood of a breach occurring.

The increase in the sophistication of cyber-attacks means that businesses must put in place adequate security to protect against cyber-attacks and data security breaches. What is adequate will come down to what is effective and should be assessed on the levels of risk and likelihood of the occurrence of a breach.

An organisation has an obligation to comply with all of the principles under data protection legislation and have measures in place to demonstrate such compliance on an ongoing basis.

If you have any concerns as to whether your business is complying or would like any other assistance with data protection, we'd be happy to help, so please do not hesitate to contact our Corporate & Commercial team by emailing Ruth.Chornolutskyy@la-law.com or calling 01202786161.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com