HFW

CABINET OFFICE HONOURS DATA BREACH: A REMINDER TO LOCK UP YOUR PERSONAL DATA

The UK Government's Cabinet Office made headlines for the wrong reasons recently after accidentally publishing personal address details of recipients of New Year honours online.

For about one hour on the evening of Friday 27 December 2019, we understand that members of the public were able to access online the full list of its 1,097 New Year honours recipients, including their personal addresses. Some of the details were sensitive enough to warrant security concerns for the individuals involved. We understand that the breach was reported to the UK Information Commissioner's Office (ICO), which is making inquiries into the incident.

The breach appears to be the result of human error, a common cause of the personal data breaches reported to the ICO. Human error is difficult for organisations to protect themselves against, especially when individuals are under pressure to deliver. However, given the damage that can be caused by a moment of carelessness, it is vital that all organisations build protection into their systems and procedures to prevent it. Failure to do so could result in the imposition of heavier penalties.

The incident occurred seven days after the ICO had fined a London pharmacy £275,000 for "careless" storage of patient data at its premises, and five months after the ICO had announced its intention to fine British Airways and Marriott International, Inc £183,390 million and £99,200 million respectively for data breaches. Security of personal data is clearly (and rightly) a key concern for the ICO, and should be a top priority for all organisations.

Whilst the Cabinet Office, British Airways and Marriott International breaches all involved digital breaches of personal data, the pharmacy breach involved paper records. On investigation, the ICO found that Doorstep Dispensaree Ltd, which supplies medicines to customers and care homes, left approximately 500,000 documents in unlocked containers at the back of its premises in Edgware. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people. Some of the documents were also water damaged because they had not been sufficiently protected against the elements. The pharmacy breach highlights that organisations need

to pay attention to physical records as well as digital records, and that accidental loss, destruction or damage to physical records is just as much an infringement of the General Data Protection Regulation (GDPR) as to digital records.

All of this highlights the importance of ensuring that staff are fully trained in keeping personal data secure, and that privacy concerns are ingrained into day to day operations and systems of all organisations. It is also a reminder that all organisations must be aware of what constitutes a personal data breach, how to avoid them and when and how to report such breaches.

For a quick video guide on how to deal with data breaches, please see https://www.hfw.com/Video-GDPR-Data-Breaches, or find out more by contacting:

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

FELICITY BURLING
Associate, London
T +44 (0)20 7264 8057
E felicity.burling@hfw.com

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our EU, competition and regulatory trade capabilities, please visit hfw.com/EU-Competition-and-Regulatory

hfw.com

Americas | Europe | Middle East | Asia Pacific