13 April 2018 No. 165

3HR Legal Weekly

Commercial

Personal Data Breaches under the GDPR

With only weeks until the General Data Protection Regulation ('GDPR') comes into effect on 25th May 2018, businesses are rushing to comply with the requirements of the new rules. The Information Commissioner's Office ('ICO') has substantial enforcement powers, notably the right to fine the companies in breach of GDPR up to 20,000,000 Euros or 4% of their annual worldwide turnover, whichever is greater. Given the media attention on high profile breaches of personal data in recent years in the UK, we consider that the ICO will not shy away from testing the extent of its new powers. It is now time, more than ever, to seize the opportunity to meet the standards of the new requirements and guard your business against the ever-increasing threat of personal data breaches.

What is a personal data breach?

A personal data breach under the GDPR relates only to breaches of personal information, as opposed to trading or organisational data. This means any information relating to an identified or identifiable natural person. A breach of security will be a breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data. This can occur in various ways:

* loss, damage or theft of device on which the data is stored;
* unauthorised access to data due to lack of security restrictions;
* deliberate attacks on systems such as hacking, scams or viruses; or
* accidental deletion or alteration of data.

Any of these breaches can put the rights and freedoms of the impacted individuals under serious risk. They can be made vulnerable to identity theft, fake transactions under their name, or fraud resulting in damage to their reputation, and putting them at risk of discrimination or financial loss.

Requirements under the GDPR for data controllers and processors

If you are a data controller but outsource some or all of your data to be processed by third parties in the UK or overseas, you will remain responsible for the overall protection of the personal data. Therefore, it is important that you adopt appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These can include:

* the pseudonymisation and encryption of personal data;
* the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
* the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
* a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; and
* proper policies and staff training.

Notifying the breach to the ICO

One of the major changes brought by the GDPR will be a duty placed upon all businesses to report personal data breaches to the ICO. Any such breach must be reported to the ICO without undue delay but at the latest within 72 hours after becoming aware of the breach occurring. In some circumstances, notice will also have to be given to the individuals affected by the breach of their data. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Time is running out. Should you require any assistance in this or any other commercial area please refer to our 3HR Commercial Law team which can advise accordingly.

Richard Hull
Commercial Solicitor
E: richard.hull@3hrcs.com