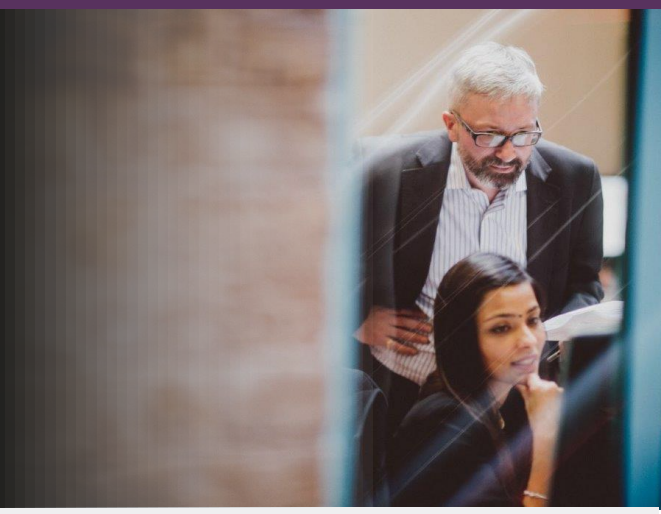
RIAA Barker Gillette

*Always Available*

# Businesses face bigger penalties on data leaks



**January 2018**

**Businesses are on a final countdown to the introduction of the General Data Protection Regulation in May 2018, bringing with it tighter rules and greater penalties for data processing, and the outcome of a landmark High Court case has made the preparation even more pressing.**

The case involved an online leak of payroll data by Andrew Skelton, a disgruntled ex-employee of supermarket chain Morrisons. Skelton received an eight-year conviction for offences under the Computer Misuse Act 1990 and the Data Protection Act 1998. However, over 5,000 current and ex-employees later joined together to bring a claim against the company itself, with the court finding Morrisons liable for the actions of its former member of staff.

The data included salary and bank details of some 100,000 staff and the ruling, which is the first data leak class action in the UK, allows those affected to claim compensation for the "upset and distress" caused.

Although Morrisons has said it will appeal, experts are predicting that the judgement of vicarious liability will make General Data Protection Regulation (GDPR) compliance even more pressing for both employers and suppliers of contract labour where data processing is involved.

"*This judgement is of huge importance, because Morrisons was held liable for the criminal misuse of third party data by an employee based on the principles of vicarious liability. The impact extends beyond the claims for compensation from employees, it's also the impact on reputation and the financial and physical resources involved in dealing with the data breach. Reportedly, Morrisons spent more than £2m in responding to the misuse,"* explains corporate lawyer, Veronica Hartley.

*"Data breach is a growing worry for a business, whether relating to employees or customers, and it is set to be even higher on the agenda in the new environment of GDPR post-May 2018."*

Bringing in a tough new era in EU-wide data protection law, the GDPR will replace the UK's 1998 Data Protection Act, with new powers for data regulators and much stricter operating boundaries for businesses that process personally identifiable information about individuals.

One of the key new requirements under GDPR is the accountability principle which requires businesses (data controllers) to demonstrate compliance by showing the regulator (in the UK, the Information Commissioner's Office – the ICO) and individuals, how they comply with these new obligations.

The aim is to harmonise data protection across all EU member states by making it simpler for everyone, including non-European companies, to comply, but it brings greater responsibilities for data controllers and data processors and big penalties of up to 4% of worldwide turnover or €20 million (whichever is the greater), for non-compliance.

The biggest change is that the GDPR applies to any business processing personally identifiable information about EU citizens. This means that any UK business that is trading with EU citizens before or after Brexit will be affected, as will anyone who transfers personal data from the EU to the UK for processing or storage.

"*The Government has said that GDPR compliance will be the minimum standard in UK law post-Brexit, to enable UK companies to do business across Europe,*" added Veronica. "*Anyone who hasn't already embarked upon the GDPR journey needs to do so as a matter of urgency, as every business and organisation is affected, no matter*

*their size, and must be able to demonstrate they are complying, not just dealing with problems after they occur. While it's likely that most will need some specialist expertise on the legal technicalities and IT processes, as a starting point there is some excellent preparatory guidance on the* ICO's *website.*"

GDPR provides stronger protection for individuals in terms of consent. In place of the previous 'opt out' approach, organisations must secure positive consent from individuals for their data to be collected. The consent can be withdrawn at any time, as individuals have 'the right to be forgotten' and can also transfer their data elsewhere if they choose. Where data is to be processed for a purpose beyond that for which it was originally collected, there will need to be fresh consent. There are strict rules around data relating to children under 16 and requirements for parental consent.

The organisation will also have to provide more information about how data will be used and how long it will be kept for, as data must not be held for any longer than necessary. If data will be stored outside the EEA, details must be provided, including what safeguards will be in place.

There is a distinction between controllers and processors of data. The controller determines the process and means of processing personal data, where a processor acts on behalf of the controller. However, each has obligations in the event of a breach or lack of compliance. For an organisation that sub contracts its processing, there is a high duty of care imposed in selecting their data processing provider with procurement processes to be followed and regular ongoing reviews once appointed.

Under GDPR there will be a statutory obligation to notify the regulator – the ICO in the UK – of any breach, if an individual's personally identifiable information is at risk as a result. Fines can range up to a maximum of €20m, or 4% of total worldwide turnover for businesses, for serious contraventions.

**Veronica Hartley**
**020 7299 6922**
**veronica.hartley@riaabg.com**
**www.riaabarkergillette.com**