Cyber and Information Law Newsletter: Issue 1 - Sector spotlight

Published 30 April 2019

Spotlight on data protection issues in the employment sphere

HR professionals handle a wide range of issues from managing organisational change and employee relations processes, to leading diversity initiatives and defending employment tribunal litigation. Since May last year HR professionals have also been grappling with handling employee data in accordance with the GDPR. There have been four key areas of change since the GDPR was implemented. Here's a glimpse into these issues to which we will return in more detail in future editions of this newsletter.

First, as widely predicted, there has been a sharp increase in the number of employees submitting data subject access requests or DSARs. Often these are submitted in the context of an internal grievance or as part of wider employment litigation. One development we were not expecting is that since the implementation of the GDPR, just occasionally a data subject has made a DSAR just because they are curious to know what data their employer holds on them! Anyone who has been involved in replying to a DSAR will know how time consuming and labour intensive this exercise can be. Employers are needing to put resource into managing more DSARs, whether through upskilling staff to handle them in house or outsourcing them. It is also important to train those on the front line on how to spot a DSAR, as this may not always be obvious.

The other way in which employers have had to adapt their approach since May 2018 is keeping in mind the need to notify the ICO of employee data breaches in more circumstances than before. This is as a result of the test for notifying the ICO being set lower than before; the requirement is to notify the ICO unless the breach is unlikely to result in a risk. Classic accidental mistakes that the ICO will now need to be notified about include sending emails to the wrong employee by mistake, particularly if that email contains any reference to the intended recipient's health. While asking the actual recipient to delete the email is good practice, in the post-GDPR world this is not enough. Employers also need to think strategically about whether to notify the ICO as given the low threshold it will be the exceptional organisation that has not notified the ICO of any employee data breaches nearly one year on from the GDPR being implemented. Happily the ICO's notification form is straightforward.

A third challenge for employers since May last year has been whether their employee privacy notices are sufficient for how employee data is being handled on the ground. One key aspect of this has been in the area of monitoring and/or accessing employee emails. Some employers have found that despite their best endeavours in the run up to GDPR, their privacy notices have not quite reflected the reality in detail. This includes when, why, by whom and how monitoring is undertaken, as well as who ultimately has access to the information gathered. Ensuring any gaps are identified and plugged by recording the reasons for employee monitoring in a legitimate interest assessment form as well as updating the employee privacy notice if necessary are important first steps for employers who have found themselves in this scenario.

The final theme emerging around GDPR in the workplace has been an increase in erasure/rectification requests from employees, sometimes after a DSAR. These expanded rights are being used as a tool to expunge unfavourable disciplinary records and otherwise to secure a "clean" reference. An employer is not always obliged to comply with a request on this basis, but the grounds for refusal are complicated and must be carefully considered.

The employment and pensions group are dealing with all these issues on a weekly basis. For more information please contact Khurram Shamsee, Partner and Head of London Employment or Ceri Fuller, Practice Development Lawyer.

Authors

Khurram Shamsee

Ceri Fuller

Spotlight on data protection issues in the tech sphere

Rarely a week goes by without some interesting developments in the interaction between data protection law and technology. This can range from a big tech company being investigated for its inappropriate uses of personal data to exciting announcements about a new technology, which in itself can raise questions about personal data.

It's a fascinating and evolving area of law. It encompasses advances in modern cultural, which not only play a large part of the work we do at DACB, but also affects our personal lives. Below we explore a few key topics which have been a theme of recent months, crystal ball gazing to look ahead to what further developments may arise during 2019 and a highlight of interesting tech projects which the DACB team have been involved in and which data protection has been a key feature.

Big tech and privacy

The GDPR has given the regulators greater power to force companies to comply with the law and to heavily fine those who repeatedly or flagrantly breach it. Increasingly we are seeing the regulators turn their attention (some may say their wrath) towards the big tech companies, who to date had treated personal data as an asset which they could exploit for their own commercial advantage. One example of how a European regulator has taken action is the recent ruling against Google LLC (for more information see this article). More locally, the ICO is continuing its investigation against Facebook and Cambridge Analytica – whilst the outcome of this investigation is yet to be determined, one thing is clear, these companies are now under significant scrutiny from the regulators and indeed the media. It will be interesting to see how these companies adapt their technology and procedures to enable them to continue to offer cutting edge solutions whilst acting in the confines of data protection laws.

Looking forward - AI and Blockchain

Artificial intelligence, driverless cars, the internet of things, Blockchain - these are all examples of cutting edge technologies in which personal data is used.

Blockchain, for example, has potential to transform entire industries, such as banking, logistics and healthcare and the ICO has advised that it is currently compiling guidance on Blockchain. One of its key features is that it creates a permanent immutable record of every transaction, storing personal data in the ledger indefinitely. This directly conflicts with the GDPR principle that data should be stored for no longer than is necessary.

Interestingly, in the ICO's Information Rights Strategic Plan 2017-2021, they emphasised that they will work with tech developers and innovators to ensure privacy enhancing techniques and tools are built in to evolving technology by design. They are also keen to keep abreast of evolving technologies, enabling them to anticipate the need for guidance on particular issues. It will be interesting to see the balance the ICO tries to strike between the two competing interests once it publishes its technology strategies.

Work which DACB are involved in

DACB have a dedicated team of data protection lawyers who advise technology companies across a range of sectors – including health, retail, insurance, media and banking to name a few. Over the last couple of years, we have been working closely with these companies to help them prepare for the GDPR, running training workshops, carrying out internal audits and remediating standard policies and contracts. Some interesting projects we are involved in include:

- Working with NHS Digital on the legal aspects to the new NHS app, which enables members of the public to access their health records and book GP appointments online;
- Supporting a client who uses Facebook to collect personal information to pass on to corporate organisations who pay the individuals on Facebook to promote their products; and
- Presenting at the ICO's "citizen's jury" on AI.

Author

Christopher Air

Spotlight on data protection issues in the health sector

Technology and all things digital have been front and centre within the health sector recently. There has been a real focus on making use of technology to improve care, as well as to try and realise efficiencies and make cost savings.

We've recently seen NHS Digital's roll-out of the new NHS app, on which we provided information governance advice and support. The app provides a simple and secure way for patients across England to access healthcare services on their smartphone or tablet, allowing patients to view their health records, book GP appointments, as well as confirm their data

sharing and organ donation preferences. The app has the potential to revolutionise healthcare, by making services more accessible to patients and allowing them to update their data preferences at the touch of a button.

The outcome of the Topol Review has also been published, which considers how technological and other developments (such as including genomics, artificial intelligence, digital medicine and robotics) are likely to impact health and social care staff. The focus is on preparing the healthcare workforce for these digital changes. The review reiterated the importance of ensuring that a legally enforceable and effective data governance framework is in place, and that any data sharing is responsible and ethical.
We also saw the publication of the NHS Long Term Plan earlier this year. As envisaged by the Topol Review, the broad vision is to make digitally-enabled care mainstream across the NHS. Alongside the Government's Code of Conduct for Data-driven Health and Care, published towards the end of 2018, this should be seen as a consistent aspiration to embrace the benefits of technology. Commissioners and providers, including those in the medical technology sector, now have clearer opportunities than ever before to turn the NHS into a modern, cutting-edge service. For more information about the NHS Long Term Plan and its data initiatives, you can read our article here.

The focus on the use of technology provides a great opportunity to drive forward innovation and excellence within healthcare. However, with these opportunities also comes information governance challenges. Patient data is at the very heart of the health sector and many of you will recall that previous data initiatives within the sector have led to failure due to lack of transparency and trust. It is therefore imperative that organisations ensure that any new changes are handled sensitively and transparently. If you require any support on issues such as these, please feel free get in touch with our specialist health sector information governance team.

There has also been a recent case which has emerged in the field of medical negligence whereby a Dutch surgeon was successful in a legal action against Google Inc to remove search results relating to a website containing an unofficial 'blacklist of doctors' and which included the surgeon's name. For further information about this, please click here.

Author

Sophie Devlin

Spotlight on data protection issues in the financial services sector

Artificial Intelligence and Financial Services

Leaving Brexit aside for a few paragraphs, the data protection topic of the year to date for the financial services industry has been compliance of its use of Artificial Intelligence with data protection laws. Of course artificial intelligence has been used for years for risk assessment and fraud detection, serenading under the names of big data. In 2019 however it seems to have had its second coming with the regulators showing some concerted interest. The ICO and National Institute for Health Research-funded Greater Manchester Patient Safety Translational Research Centre jointly commissioned a Citizens Jury to gain insight into public perception about artificial intelligence and whether they think:

- people should always get an explanation for an AI-generated decision, even if that means the AI will not reach such accurate conclusions; and
- when and why explanations for AI-generated decisions are important.

Our Rhiannon Webster participated in the jury as a legal expert on the current laws regulating AI. The findings of this research will feed into guidance being produced jointly by the ICO and The Alan Turing Institute that will give organisations a steer about how they can explain AI to users.

This month, Lloyd's has published two reports exploring the trends in AI within the insurance industry. It analysed the associated risks of AI implementation as well as the potential for AI to help insurers improve their operations.

The report identifies four risks areas for AI: trust and transparency, ethics, security and safety. As artificial intelligence systems become more complex, cyber breaches are likely to have an even greater impact, according to the report. Meanwhile, ambiguity and legal uncertainty is contributing to unanswered questions around who is ultimately liable when something does go wrong.

The reports can be accessed here.

FCA and ICO sign new MOU

In February, the ICO and the Financial Conduct Authority ("FCA") updated their Memorandum of Understanding ("MoU"). The purpose of the MoU is to capture the general principles of collaboration between the parties, with the ultimate aim of

developing cooperation and knowledge sharing, resulting in a more cohesive approach to investigations.

The broad principles contained in the MoU are set out below:

- Each party agrees to alert the other to potential breaches of the legislation that the other regulates and to provide necessary supporting information (insofar as legal or procedural restriction on disclosure will permit).
- The parties will liaise with each other on a regular basis to discuss matters of mutual interest and to address common issues and threats. This may include information relating to:
  - Investigations and relevant action taken against a person or a firm by one party, which may be relevant to the functions of the other;
  - Criminal fraudulent other activity that other might cast doubt on the fitness and propriety of an FCA authorised firm, certified individual or approved person; or
  - Intelligence held by the ICO which indicates possible failures of FCA authorised firms' regulated activities (including systems and controls).
- Both parties may request relevant information from each other and if information is gathered by one party which deemed to be materially relevant to the other, notification will be provided in order to allow the other party to request disclosure of such information;
- The parties will consult and co-ordinate (where appropriate) in respect of reviews, cause for evidence and recommendations; and
- In the event of a major incident of mutual interest at an FCA-regulated firm, the parties will work together in line with an agreed incident protocol in order in order to secure the best outcome for consumers, and ensure incidents are dealt with in a coordinated and efficient manner.

Whilst the MoU does make reference to one party taking "the lead" in an investigation if appropriate, it also clearly recognises that there are circumstances where it will be appropriate for both the ICO and the FCA to investigate and take enforcement action. FCA authorised firms should continue to prioritise data protection compliance in order to stay on the right side of both regulators.

For further information the MoU can be accessed here.

Authors

Rhiannon Webster

Jade Kowalski

Authors

Ceri Fuller

London - Walbrook
cfuller@dacbeachcroft.com

Khurram Shamsee

London - Walbrook
kshamsee@dacbeachcroft.com

Jade Kowalski

London - Walbrook
jkowalski@dacbeachcroft.com

Sophie Devlin

Newcastle
sdevlin@dacbeachcroft.com

Christopher Air

Manchester
cair@dacbeachcroft.com