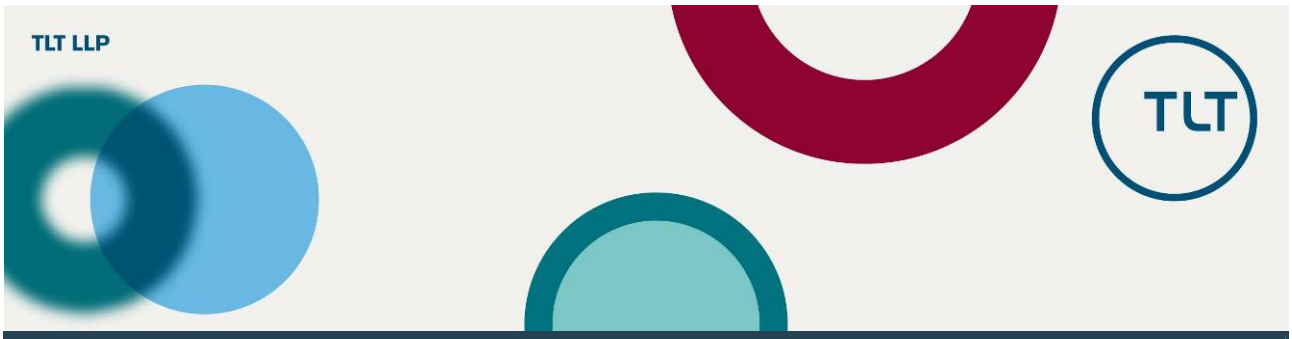

TLT data protection news September 2015

This edition in summary:

- Ashley Madison - Life is short: comply with your data protection obligations!
- Subject access requests: reasonable and proportionate searches
- Target Corp and Visa Inc reach US$67 million settlement following dataset hacking
- ICO publishes its comments on the EU Regulation
- Enforcement notice against Google
- The risks of direct marketing lists
- ICO guidance on crime and taxation exemption
- Privacy campaign group's report highlights local authority data breaches
- Summary of ICO actions

Ashley Madison - Life is short: comply with your data protection obligations!

As the majority of readers are no doubt aware, the big news in the data protection sphere over the last few weeks has been the extremely highly-publicised data breach suffered by dating website Ashley Madison. The website, owned by Canadian company Avid Life Media, was set up to facilitate participation in extra-marital affairs and has a user base of around 40 million.

Most of those 40 million users were affected by the breach and it is estimated that 1.2 million of these users are based in the UK. Despite this, it is not clear whether the UK legislation, the Data Protection Act (**DPA**), or equivalent legislation implementing the European Data Protection Directive (the **Directive**) would apply to Ashley Madison, given that the website's owner is based in Canada.

If the DPA does apply to Ashley Madison, it is beyond doubt that the site has committed numerous breaches of the legislation. In particular, it has been criticised about the level of security measures taken in view of the sensitive nature of the information. It also appears to have fallen down on the accuracy of the personal information held and the length of time it retains individuals' personal data. We consider each of these issues further here.

The message to take away from the Ashley Madison case is clear: data protection breaches can not only be catastrophic for a business, but can be life-changing for individuals as well. In light of the Ashley Madison breach, organisations, particularly those who handle sensitive personal data, would be well-advised to review their security measures, verification systems and retention policies to avoid becoming the next data breach victim and the financial and reputational consequences that inevitably follow.

Subject access requests: reasonable and proportionate searches

Often data controllers will receive requests for personal data where the data subject is in litigation or impending litigation with either the data controller or a third party. This often causes friction between the lawyers handling the litigation and the individuals responsible for responding to the request.

In the case of *Dawson-Damer & others v Taylor Wessing & others*, the High Court re-affirmed previous judgments when it refused an application under s7(9) of the DPA for an order to compel the defendant to comply with a subject access request. This was because the court felt that the request was made for the primary purpose of assisting a litigation case.

The first issue that the court had to consider was the scope of legal privilege. The court determined that legal privilege, for the purposes of subject access requests, should have the same meaning as in litigation.

The court also had to consider whether the search requested was reasonable and proportionate. The defendant had refused to undertake a detailed and extensive search for the applicant's personal data on the grounds that, as the majority of the personal data held was legally privileged, it would not be reasonable and proportionate to undertake a search to locate any non-privileged personal data. The court agreed with the defendant on the basis that this would be a particularly expensive and lengthy exercise (involving skilled lawyers) to determine which documents were protected by privilege.

Whilst the court supported the defendant's approach in this case, the decision should not be seen as a blanket exemption from undertaking any searches in the context of impending civil litigation. It is worth noting that the decision is being appealed to the Court of Appeal so the position may be reviewed further. For more detail on the Dawson case and other case law on this topic, please click here.

Target Corp and Visa Inc reach US$67 million settlement following dataset hacking

In 2013, Target's databases were hacked and the personal data of 110 million of its customers (including the credit card details of 40 million customers) was stolen. In the immediate aftermath the CEO of Target resigned, citing that he felt personally responsible for the breaches.

Visa Inc brought a claim against Target in conjunction with a number of issuing banks who incurred costs in relation to the data breach (such as the costs of reissuing credit/debit cards). The US judge had stated that it was at least arguable that Target was under a duty of care to the financial institutions and that it had breached this duty.

A claim made by MasterCard is still ongoing as the issuing banks previously rejected a US$19 million settlement offer by Target. Alongside these claims by financial institutions there are also claims being brought by consumer groups.

Visa and Target announced earlier this month that they have reached a settlement. This settlement is reported to be in the region of US$ 67million and is subject to acceptance by the issuing banks. As part of the settlement, it is understood that issuing banks that accept the offer will not be able to take further action against Target for these costs.

Although this action is going on in America, the implications of a large data breach would be similar in the UK, with card issuers increasingly likely to look to retailers, or other organisations, to recompense them for losses caused by data breaches.

ICO publishes its comments on the EU Regulation

Further to the European Council reaching a 'general approach' on the General Data Protection Regulation (**Regulation**) in June, the ICO has now published its commentary on the Council text. It sets out areas where it considers that there is greatest need for improvement during the trilogue process, which is now well underway.

The European Parliament has published a roadmap for the trilogue discussions up to December 2015. This has been described as 'the last mile of a marathon effort' to reform the data protection regime. However, in its recent blog, the ICO considers that, on the most optimistic forecast, the two year run in period is unlikely to start much before June 2016. This will mean that the Regulation will not be in force until June 2018, but the end of 2018 may be more realistic.

Christopher Graham, the Information Commissioner, has said in a recent interview that the changes haven't happened quickly enough. He also expressed concern about the prescriptive nature of the legislation in terms of process for data protection authorities. In particular, he does not think it is helpful for the Regulation to dictate that the ICO must fine for every breach. Instead, he thinks that data protection authorities should be given discretion to take risk and proportionality into account. Of particular interest is his comment that he's been told by the European Commission that he will 'only need to fine one euro'. This appears to indicate a

significant softening in the Commission's approach. However, Christopher Graham would prefer to jump on the breaches causing most damage, rather than tying up the ICO's resources on issuing one euro fines.

The ICO has stressed throughout the process that the final text should be "clear, simple and easy to understand" if it is to have the desired effect of improving privacy protection in practice as well as on paper. This plea has been echoed by the European Data Protection Supervisor in their recent opinion entitled "Europe's big opportunity".

Christopher Graham has likened the Regulation to a shopping list at the moment containing every best practice idea that anyone has ever had. Whether or not this shopping list will be simplified, or grow even longer as the trilogue discussions progress, remains to be seen.

Enforcement notice against Google

In issuing its first enforcement notice relating to the 'right to be forgotten', the ICO has ordered Google Inc to remove eight links to news articles about a person's criminal offence committed nearly a decade ago.

The enforcement notice comes just over a year after the European Court of Justice (**ECJ**) ruled that EU citizens have the right, in response to a search for their name, to request internet search engines to remove outdated or irrelevant search results. In the somewhat controversial decision in May 2014, the ECJ had ordered Google Spain to remove links referencing the criminal history of an individual after that person made a request that the links be deleted.

The recent ICO decision is particularly interesting as, unlike the Google Spain case, it does not directly relate to the delisting of data about an individual. Instead it concerns the removal of links to news articles about the actual delisting decision that were displayed when a search was made against that individual's name. Although Google Inc had agreed to remove a link to a website containing a report about the complainant's criminal offence, it then refused to delist links to eight other webpages that contained news articles about its removal of the original link, and included the information about the complainant's criminal offence.

Google Inc tried to argue that the links to the news articles were relevant and in the public interest. The ICO did not dispute that the stories might be newsworthy and in the public interest, but, in its view, this did not justify keeping available links to those stories when an individual's name is searched, because this negatively impacts the individual's privacy and breaches the DPA.

The ICO stated that the case did not concern an individual in public life, and there was no wider public interest in making the information publicly available. The information was sensitive personal data and, being almost a decade old, was not reasonably current. The individual's previous conviction was for a relatively minor offence which was spent, and therefore the ICO considered that making the information publicly available had a disproportionately negative effect on their privacy.

Accordingly, the ICO concluded that Google Inc had breached the DPA on two grounds:

- That it had not processed personal data fairly and lawfully; including complying with at least one of the schedule 3 conditions (which governs the processing of sensitive personal data, including information about criminal convictions); and

- That the personal data it processed was not adequate, not relevant and excessive in relation to the purpose and purposes that they were being processed.

Google Inc was ordered to remove the links from its search results in response to a search for the individual's name within thirty-five days of the date of the enforcement notice (18 August), or risk facing further enforcement action. Google has a history of refusing to comply with enforcement notices issued by data protection authorities and therefore it remains to be seen whether Google Inc will invoke its right to appeal against the ICO's enforcement notice.

It is likely that we will start to see more and more 'right to be forgotten' cases, where individuals request the removal of outdated or irrelevant information. This will have an impact not only on internet search engines, but potentially any websites containing links or searching functions, social media and online blogs.

The risks of direct marketing lists

Direct marketing is a highly sensitive and high profile topic at present. The Information Commissioner has recently issued several enforcement notices and brought criminal prosecutions against organisations that

have breached the DPA and, in the case of electronic marketing, the Privacy and Electronic Communications Regulations (**PECR**). There has also been a recent spate of media stories about charities and other organisations buying and selling individuals' details which has led to three separate investigations by not only the Information Commissioner but also by a parliamentary select committee and the Cabinet Office.

In light of the recent media coverage, the ICO has launched a review of its guidance for organisations carrying out direct marketing activities. This includes guidance on the PECR and the buying and selling of personal data. This guidance was last updated in 2013 and the ICO has published a survey to measure how often organisations refer to the guidance document, how easy it is to understand and how useful organisations find it.

A recent Information Tribunal decision on the issue of direct marketing also highlighted the risks for organisations when using marketing lists. In this case, Optical Express, sought to challenge the enforcement notice issued by the Information Commissioner last December in respect of unsolicited marketing texts sent to recipients on a third party marketing list. The Information Tribunal rejected the appeal and confirmed that the burden of proof for an alleged breach of direct marketing legislation lies, not with the Information Commissioner as Optical Express had suggested, but, instead with the organisation to show that it has complied with the legislation.

This case highlights the need, when buying in marketing lists, to undertake a check on what the individuals contained in the list have consented to. Just because an individual has consented to receive marketing communications from third parties, it does not mean that he/she has consented to receive marketing communications about every product and service under the sun.

For more information on the appeal, click here.

ICO guidance on crime and taxation exemption

Updated guidance has been issued by the ICO in relation to the 'crime and taxation exemption' under the DPA. The guidance can be found here.

Under section 9 of the DPA, personal data may be used in ways which would normally contravene the data protection principles if it is for one or more of the following purposes:

- the prevention and detection of crime;
- the apprehension or prosecution of offenders, or
- the assessment or collection of tax.

For example, data controllers processing data for the relevant purposes may withhold information that should usually be provided to individuals and/or disclose personal data in ways that would otherwise breach the data protection principles, if it is necessary for the relevant purposes.

However, it is not always straightforward to know whether this 'crime and taxation exemption' applies.

Part of the guidance is aimed at organisations that often process data for crime and taxation purposes, like the police and HMRC, and part is aimed at organisations that are asked to provide data to the police.

The guidance provides useful examples based on common scenarios and also contains reminders that the 'crime and taxation exemption' applies to the way personal data is used, rather than the type of organisation using it. It is important to note that even if your organisation regularly processes information for the purpose of detecting or preventing crime, not all personal data processed will fall under the scope of this exemption.

Whether or not your organisation regularly processes information for the purposes of detecting crime, or is asked from time to time to provide information to the police, the guidance is a good starting place for considering your obligations.

For more on this topic, click here.

Privacy campaign group's report highlights local authority data breaches

Privacy campaign group Big Brother Watch has released a report entitled a "Breach of Trust" highlighting that in the past three years there have been 4,236 data breaches in local authorities of varying seriousness; a number equivalent to almost four breaches a day.

Notable incidents included child protection files being left on a train and a worker using CCTV to watch a colleague's wedding.

The group is calling for harsher penalties following the finding that 68% of such data breach cases involved no disciplinary action.

To compile the report Big Brother Watch sent freedom of information requests to all UK Local Authorities. Over the period 167 town halls reported no data breaches.

Summary of ICO actions

For our round-up of recent monetary penalties enforced by the ICO, please click here.

TLT contact

Alison Deighton, Partner

+44 (0)333 006 0160
alison.deighton@TLTsolicitors.com