Data Protection and Privacy

CLYDE&CO

Newsletter

April 2013

Contents

Further lobbying against EU data protection reforms

According to an article in the **Guardian**, nine EU member states, including the UK, Germany, Sweden and Belgium, have been lobbying against some of the proposed measures in the EU's data protection law reforms that would increase compliance burdens on businesses. This follows a period of intense lobbying against the proposed reforms by companies that collect large amounts of personal data, such as Google and Facebook, and the US government.

The ICO and other EU member states sympathetic to companies' concerns regarding the proposed reforms have suggested that member states should have more freedom to interpret the law as appropriate, using a "risk based" approach to regulation, focusing on cases where there is a substantial threat to a person's data or privacy.

The article quotes an ICO spokesperson as giving the following example: "*If you have a butcher whose data processing only affects 20 local people, you need to be able to treat an infringement there differently from a company with private health records*".

Although the European Parliament is likely to oppose any watering down of the reforms, there are enough member states to block the reforms completely, which is likely to force concessions to be made.

ICO publishes guidance on "BYOD"

The ICO has published helpful **guidance** explaining some of the risks organisations must consider when allowing personal devices (so-called "bring your own device" or "BYOD" practices) to be used to process work-related personal data and ways to help ensure compliance with the Data Protection Act 1998 in connection with BYOD policies.

The ICO admits that the cost of introducing the suggested controls may be "quite significant" and might be greater than the initial savings expected through having a BYOD policy, but suggests that the sum will be insignificant if one considers the likely reputational damages flowing from a data breach.

Some of the key recommendations from the guidance are:

- Being clear on the types of personal data that can be processed on personal devices
- Registering personal devices with remote locate and wipe facilities so to allow the confidentiality of personal data to be maintained in the event of loss or theft
- Being clear with staff about which types of personal data may be processed on personal devices
- Using strong passwords to secure personal devices and ensuring that access to a personal device is locked or personal data automatically deleted if an incorrect password is inputted too many times
- Enabling encryption to store data on personal devices securely
- Using public cloud-based sharing and public backup services, which have not been fully assessed for security and other features, with extreme caution, if at all

The ICO also **published the results of a survey on BYOD practices**. The survey, commissioned by the ICO and carried out by YouGov, suggests that 47% of UK adults now use their personal smartphone, laptop or tablet computer for work purposes, but less than 30% of these users are provided with guidance on how their personal devices should be used in this capacity. The ICO states that this raises concerns that people may not understand how to look after the personal data accessed and stored on their personal devices.

Heidi Watson from Clyde & Co's Employment team has made the following comment in relation to BYODs:

"This ICO guidance highlights the dangers of allowing employees to use their own devices for work emails. The statistics show this is a common practice whilst many employers have not given thought to limiting the risks. Employers will need robust policies to ensure employees do not put sensitive data at risk and, where they breach the policies, to enable employers to take suitable disciplinary action. Whilst there are benefits to allowing employees the flexibility of BYODs, it is clear that employers need to give serious thought to whether their current data protection or e-communications policies provide sufficient protection against the inherent dangers."

Back to page 1

GP surgery receptionist fined for unlawfully accessing patient information

A receptionist at a GP surgery (the **Defendant**) unlawfully accessed sensitive medical records of her ex-husband's new partner on 15 separate occasions over a 16 month period. According to the ICO's announcement on the case, after the Defendant left her job she sent a text message to her ex-husband's new partner referring to highly sensitive medical information taken from her medical records.

The Defendant was found guilty of unlawfully obtaining personal data, which is a criminal offence under section 55 of the Data Protection Act 1998. Section 55 of the Data Protection Act 1998 sets out that a "*person must not knowingly or recklessly, without the consent of the data controller obtain or disclose personal data or the information contained in personal data*" or "*procure the disclosure to another person of the information contained in personal data*". The Defendant was fined £750 by the West Hampshire Magistrates' Court and ordered to pay a £15 victim surcharge and £400 prosecution costs. The ICO's statement on the case can be found **here**.

Back to page 1

ICO issues £90,000 fine for cold calling

Regulation 21 of the Privacy and Electronic Communications (**EC Directive**) Regulations 2003 (**PECR**) requires that, where a consumer is registered with the Telephone Preference Service (the central register run by OSCOM on which consumers can register their preference not to receive unsolicited direct marketing calls), the consumer's consent to receiving direct marketing calls must have been given to a business before it makes direct marketing calls to that consumer. Therefore, businesses involved in direct marketing by telephone should register with the Telephone Preference Service to receive a monthly update of the Telephone Preference Service's list so as to enable them to to check this list prior to making unsolicited direct marketing calls. A business should also maintain a "suppression list" of those consumers who have informed it directly that they do not wish to receive direct marketing calls.

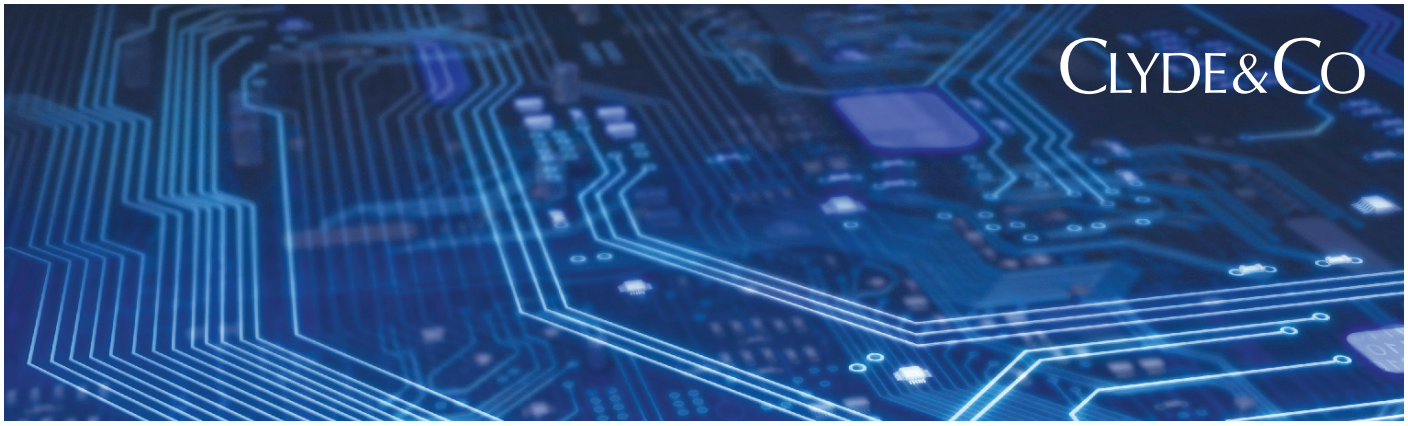
DM Design Bedrooms Limited (**DM Design**) manufactures, fits, sells and markets kitchens and bedrooms. DM Design carried out direct marketing to consumers by telephone. Between June 2011 and November 2012, the Telephone Preference Service received 1,945 complaints from consumers registered on the "do not call" list who had received unsolicited direct marketing calls from DM Design. Each of these complaints was sent by the Telephone Preference Service to DM Design inviting a response. DM Design only responded to 19 of the complaints. One complainant stated that the DM Design caller was so intimidating that she felt compelled to report the matter to the police: the DM Design caller had told the complainant that he would never remove her name from DM Design's marketing list and would "continue to call at more inconvenient times like Sunday lunchtime". Another complaint was made on behalf of an elderly woman suffering from dementia who had been the subject of a "very pushy" call.

In addition, the ICO had previously separately contacted DM Design regarding its compliance with the PECR, but DM Design failed to take steps to ensure compliance.

The Commissioner held that there had been a breach of Regulation 21 of the PECR, as DM Design had made unsolicited calls to consumers whose phone numbers were registered with the Telephone Preference Service and had not given their prior consent to DM Design to receive the calls. Given the nature, duration and extent of the breach, the Commissioner held that there had been a "serious" breach of Regulation 21 and, given the large numbers of individuals receiving the unsolicited calls and the nature of some of the complaints they gave rise to, the breach was likely to cause substantial damage or distress. DM Design was **fined £90,000**.

In the ICO's commentary on the decision it highlighted that the penalty is the first the ICO has issued for a serious breach of the PECR relating to marketing calls. According to the ICO website, the ICO has informed two more companies that it is intending to impose significant penalties for breaches of this law.

Back to page 1



Data protection impacts of the NHS reforms in England

The ICO has published a **blog post** discussing the recent NHS changes in England. According to the post, the health sector continues to be a priority area for the ICO, with the ICO in the last year having served monetary penalties totalling over £1 million on health service organisations for breach of the Data Protection Act 1998.

Under the Health and Social Care Act 2012, Primary Care Trusts and Strategic Health Authorities have been abolished and new Clinical Commissioning Groups and an NHS Commissioning Board have been created.

The ICO has been working to ensure that the new bodies, and those which have been abolished, fully understand what is required for them to comply with their obligations under the Data Protection Act 1998 and in respect of freedom of information requests.

The ICO has recommended that NHS organisations undertake, where appropriate, privacy impact assessments and that those involved in the new framework fully inform the public about what they do and be transparent about what, why, how and when they collect and use data.

The ICO has published **FAQs** to assist those involved in the transition and also for the information of the wider public.

The ICO continues to have reservations about the sharing of data between health bodies and wants to ensure that organisations understand why, when and how to share data.

There is a tension in the law, as the Health and Social Care Information Centre (the NHS' central information hub) now has the power under the Health and Social Care Act 2012 "*to require and request provision of information*" (which includes patient information held by GPs, who are the data controllers of such information), whereas under the Data Protection Act 1998 a data controller has a legal obligation to ensure that it is complying with the Data Protection Act when sharing personal data. The ICO is working with the Health and Social Care Information Centre to determine whether its power relieves data controllers from their obligations under the Data Protection Act 1998.

James Cassidy from Clyde & Co notes that "*the wholesale changes in the structure of the NHS represents a real risk area in terms of Data Protection Act compliance. The ICO has already expressed concerns about the management of data within the NHS, and the changes in organisational structure provide a further obstacle to the NHS in ensuring that personal data is processed safely and securely. New NHS organisations must quickly establish systems and processes to govern how data is managed, and existing NHS organisations should be assessing how and where data is being transferred in light of the dissolution of PCTs and SHAs.*"

Back to page 1

Apple defends privacy lawsuit in California

Apple is defending a lawsuit in California in which it is accused of improperly collecting data on the locations of customers using iPhones, even after the device's geo-location feature was turned off, and sharing personal information with third parties.

In the latest development in the lawsuit, the plaintiffs' lawyers have been **invited to pursue sanctions against Apple** for failure to comply with its document production obligations in connection with the litigation.

The plaintiffs are separately seeking permission to proceed with the lawsuit on a group basis. Apple argued that class action status should be denied because the plaintiffs have not shown that any users had personal information collected without their consent, and so cannot show that they have suffered any harm.

We will provide updates on significant developments in this litigation in future newsletters.

Google faces action by six European Union data protection authorities

The data protection authorities of France, Germany, Italy, the Netherlands, Spain and the UK have launched investigations into Google's privacy policy in light of concerns regarding its compliance with EU data protection laws. This is the first coordinated, formal procedure by EU data protection authorities against a single company on data protection issues.

By way of background, in March 2012, Google updated its privacy policy to unify more than 60 separate privacy policies across its product range. Google's changes allowed it to combine user data from its different services; for example to permit videos watched on YouTube to inform the choice of advertising shown when conducting general Google searches.

In October 2012, the European Union's data protection working party, led by CNIL (the French data protection authority), criticised Google's new privacy policy for failing to provide sufficient information to users on Google's personal data processing operations, not informing users how long their personal data would be retained and allowing the uncontrolled combination of data across Google's services. CNIL also criticised Google for being uncooperative in its responses to queries in the investigation. CNIL's **report** included recommendations for Google to improve its privacy policy and practices.

Google responded to the report by stating that its privacy policy respected European law.

Google was asked to comply with the CNIL report's recommendations within four months. However, according to a **statement on CNIL's website**, Google did not implement any significant compliance measures within this period.

In March 2013, representatives from Google met with representatives from the data protection authorities of France, Germany, Italy, the Netherlands, Spain and the UK to discuss the recommendations for changes to Google's privacy policy and practices. According to CNIL, following this meeting Google did not introduce any changes.

Therefore, the six data protection authorities have launched formal investigations regarding breach of data protection law by Google on the basis of the provisions set out in their respective national legislation.

Although, according to an **article in the Guardian**, the maximum fines that could be imposed by the UK's ICO (£500,000) and France's CNIL (€300,000) would in total be less than the amount Google generates in sales in 10 minutes, the data protection authorities could bring legal action seeking to block Google from operating in Europe, which would be damaging to Google's reputation and finances.

Back to page 1

Appeal against Monetary Penalty Notice dismissed by Tribunal

In recent months, the First Tier Tribunal has heard the first appeal against a Monetary Penalty Notice (**MPN**) handed out for a breach of the DPA. Central London Community Healthcare NHS Trust appealed against the fine of £90,000 for the accidental disclosure of patient information by fax. The Tribunal however held that the level of fine was appropriate and dismissed the appeal.

The ICO issued a MPN in April 2012 after the Trust had inadvertently faxed details of palliative care patients to the wrong fax number on 45 separate occasions. The faxes had been sent to a member of the public who notified the Trust of the error. The Trust argued that the decision of the ICO to award an MNP was not in accordance with the law, and requested that the decision to award an MNP be quashed, or the penalty be substituted for a lower amount.

In handing down their decision the Tribunal clarified the following key issues:

- The decision of a Tribunal is a "de novo" hearing, meaning that the Tribunal is to conduct a fresh hearing of the issues
- There is no duty upon the ICO to indicate whether they are considering issuing a MPN during an investigation into an incident
- The Tribunal held that voluntary notification "cannot be given much weight" as a mitigating factor when considering whether to impose an MPN
- The ICO confirmed that there is an "unpublished framework" as to the likely fines for different severities of breach:
  - Serious breach - £40,000 to £100,000
  - Very serious breach - £100,000 to £250,000
  - Most serious breach - £250,000 up to the maximum of £500,000

The breach of the DPA by the Trust was deemed to be "serious" - the lowest rung of severity on the ICO's scale, but the Tribunal upheld that the imposition and level of a fine in this matter was appropriate.

In terms of notification of the breach to the ICO, the Tribunal stated that the *"Trust was under, in effect, an obligation to report"*.

The Tribunal also confirmed that if an appeal against an MNP is lodged, the Data Controller will lose the potential for a 20% discount on the fine for early payment. The Tribunal confirmed *"The purpose of the scheme would appear to us to encourage early payment and also to ensure there is an early resolution to the matter. There is no provision for a without prejudice payment"*. Data Controllers should take this into account when considering whether to lodge an appeal. 20% is a substantial amount of money given the level of fines already being handed out by the ICO.

The decision of the FTT demonstrates that the level of fine handed out to date by the ICO will continue. With the ICO expressing a cause for concern about data compliance in the public sector, all organisations should have policies and procedures in place to ensure that data is processed lawfully. In light of the Tribunal's decision, all Data Controllers must face the reality that a serious breach of the DPA is now very likely to result in a fine of thousands of pounds.

Back to page 1

Academic calls on the UK Government to provide the ICO with the funding it requires to be effective

According to an article in The Global Legal Post found **here**, a paper presented on 11th April by Dr Karen McCullagh of the University of East Anglia reports that the ICO is, and will continue to be, 'ineffective' unless the government takes action.

Dr McCullagh's research studies the effectiveness of the ICO since its creation almost 30 years ago and she has said that these studies have led her to believe that the investigative and enforcement powers of the ICO *"have been, and continue to be, lamentably weak and ineffective"*.

Dr McCullagh added that the new proposed EU data protection regulation will not enhance the powers of the ICO if *"the UK government does not take measures to create an adequately funded and properly staffed regulatory office, with appropriate investigative and enforcement powers"*.

Back to page 1

Contributors

If you would like further information on any of the issues raised in this newsletter please contact your usual Clyde & Co contact or one of the contributors to this newsletter listed below:

Alan Meneghetti
Partner, London
T: +44 (0)20 7876 5616
E: alan.meneghetti@clydeco.com

Andrew Horrocks
Partner, London
T: +44 (0)20 7876 6511
E: andrew.horrocks@clydeco.com

James Cassidy
Senior Associate, London
T: +44 (0)20 7876 6081
E: james.cassidy@clydeco.com

Isabel Ost
Associate, London
T: +44 (0)20 7876 5313
E: isabel.ost@clydeco.com

Heidi Watson
Legal Director, London
T: +44 (0)20 7876 4480
E: heidi.watson@clydeco.com

Clyde & Co offers international coverage on data protection and is well placed to provide an immediate response to data breaches and cyber threats wherever they occur. Our experienced data protection and privacy team spans our global network of offices across Europe, the Americas, Asia-Pacific and the Middle East - advising on a wide range of data protection and privacy issues.

Clyde & Co LLP
The St Botolph Building
138 Houndsditch
London EC3A 7AR

T: +44 (0)20 7876 5000
F: +44 (0)20 7876 5111

Further advice should be taken before relying on the contents of this summary.

Clyde & Co LLP **www.clydeco.com**

Back to page 1