Data Protection Newsletter

www.regulatorystrategies.co.uk

April 2018

Headlines this month:

- Data protection standards to be maintained post-Brexit
- ICO publishes introduction to Data Protection Bill
- ICO confirms consent needed for electronic marketing
- Affiliate Marketers under scrutiny
- ICO releases 'Making data protection your business' guidance
- DP Bill amendments on data processing for safeguarding purposes
- New UK data protection registration fee
- Article 29 Working Party GDPR guidance
- WhatsApp signs undertaking with ICO
- ICO investigation into data analytics for political purposes

Commentary:

Data protection standards to be maintained post-Brexit

Theresa May, Prime Minister, spoke about data protection law as part of her major policy speech in London on all aspects of Brexit on 2 March.

She said "the free flow of data is also critical for both sides in any modern trading relationship too. The UK has exceptionally high standards of data protection. And we want to secure an agreement with the EU that provides the stability and confidence for EU and UK business and individuals to achieve our aims in maintaining and developing the UK's strong trading and economic links with the EU.

"That is why we will be seeking more than just an adequacy arrangement and want to see an appropriate ongoing role for the UK's Information Commissioner's Office. This will ensure UK businesses are effectively represented under the EU's new 'one stop shop' mechanism for resolving data protection disputes."

In her speech Theresa May cited data protection as one of the "five foundations" of the future relationship between the UK and the EU.

ICO publishes introduction to Data Protection Bill

The ICO has published an introduction to the **Data Protection Bill** (DPB). The ICO will publish more detailed guidance once the DPB has been enacted.

This initial introduction serves mainly to set out the structure and content of the draft legislation. The sets out the effect of the various sections of the Bill, the extent to which it represents a change, and the reason the change is required.

It also sets out the derogations under the GDPR at a high level.

ICO confirms consent needed for electronic marketing

The Information Commissioner has confirmed in a speech to the Direct Marketing Association, that until further notice, consent will be required for electronic marketing under PECR which will sit alongside the GDPR.

The draft ePrivacy Regulation currently proposes opt-in as a default for all consumer marketing. The ICO said that there is some potential to use legitimate interests as a legal basis for processing "but you must be confident you can rely on it".

She went on to say: "It seems to me that a lot of energy and effort is being spent on trying to find a way to avoid consent. That energy and effort would be much better spent establishing informed, active, unambiguous consent", and stressed that she thought this would lead to more effective marketing rather than to a loss of customers.

It remains to be seen where this leaves the 'soft opt-in' in respect of marketing similar products and services.

Affiliate Marketers under scrutiny

The affiliate marketing industry has been warned about areas of non-compliance with privacy and marketing law following a global intelligence-gathering operation. The operation by the Unsolicited Communications Enforcement Network, involved nine agencies from five countries looking at 902 websites and examining 6,536 consumer complaints.

Affiliate marketing is a commercial arrangement allowing a company to generate business by allowing other organisations ("affiliates") to promote their products or services. For example, an online retailer may pay commission to an external website for traffic or sales generated from its referrals, by hosting links on its own site or sending links out via email or text message.

ICO releases 'Making data protection your business' guidance

The ICO has published guidance for 'micro' businesses and sole traders on GDPR compliance. The guide offers eight steps businesses should take to meet GDPR requirements including:

- **Make sure you have a record** of the personal data you hold and why.
- **Identify** why you have personal data and how you use it.
- **Have a plan** in case people ask about their rights regarding the personal information you hold about them.
- **Ask yourself: before I collect their data,** do I clearly tell people why I need it and how I will use it?
- **Check your security**. This can include locking filing cabinets and password-protecting any of your devices and cloud storage that hold your staff or customers' personal data.
- **Develop a process** to make sure you know what to do if you breach data protection rules.

As part of the guidance, the ICO says:

A common myth is that the ICO will be fining organisations large sums for every breach of data protection law. Please remember: the ICO is here to uphold the information rights of the UK public. We can and do fine organisations, but we have other tools at our disposal to ensure that businesses comply with the law. ***Monetary penalties have been and will continue to be a last resort of our regulatory action*** *– our primary aim is to support businesses to get things right and improve their practices where required.*

DP Bill amendments on data processing for safeguarding purposes

The House of Commons Public Bill Committee has adopted government amendments that introduce new measures for processing personal data for safeguarding purposes.

Amendment 85 covers processing that is necessary for protecting children and vulnerable adults from neglect or physical or mental harm. This addresses the gap in relation to expectations, for example, on sports governing bodies. The amendment permits the processing of sensitive personal data, which is necessary to safeguard children from physical, emotional, sexual and neglect-based abuse.

Amendment 86 deals with a related issue where processing health data is necessary to protect an individual's economic wellbeing, where that individual has been identified as an individual at economic risk.

For example, banks occasionally need to record health data without the consent of the data subject. An example was given of a bank which was contacted by a family member who was alerting the bank to an elderly customer suffering from mental health problems who was drawing large sums of money each day from their bank account and giving it away.

New UK data protection registration fee

A new data protection registration will apply in the UK from 25 May 2018.

While the incoming General Data Protection Regulation (GDPR) does away with an annual notification requirement, it also increases the tasks which need to be carried out by Supervisory Authorities, all the while, doing away with the income they receive from notification fees. Recognising the need for increased revenue, the UK government has decided this will be partially funded by a new annual data protection fee which will replace the current notification fee.

There are three tiers of fees: £40, £60 and £2,900. The fee payable will depend on how many members of staff an organisation has, its annual turnover, and whether or not it is a public authority, a charity or a small occupational pension scheme. Some data controllers will be exempt from registration fees.

- Tier 1, micro organisations - £40: maximum turnover of £632,000 for the financial year OR no more than ten members of staff;
- Tier 2, small and medium organisations - £60: maximum turnover of £36m for the financial year OR no more than 250 members of staff; and
- Tier 3, large organisations - £2900: all other eligible organisations.

Note that the ICO will regard all controllers registering for the first time (and not currently notified under the Data Protection Act 1998) as eligible to pay a Tier 3 fee unless and until it is told otherwise.

The ICO will publish a self-assessment tool before the Regulations come into effect. If an organisation is already registered under the 1998 Data Protection Act, the ICO will decide what Tier is applicable and organisations have the right to object. An organisation paying a fee for the first time will need to inform the ICO of its name, contact details, and which level of fee it thinks it will need to pay. A telephone line has been set up to take this information which can also be submitted online.

The ICO will collect the following information from all registrants:

- name and address of controller and other trading names;
- number of staff;
- turnover for financial year; and
- contact details for: person completing the registration process; person responsible for regulatory issues and renewal of registration fee if different; and the DPO (if there is one).

Information which the ICO will publish will be limited to:

- name and address of controller (but not individual contacts);
- data protection registration number allocated by the ICO;
- level of fee paid;
- date of fee payment and renewal date; and
- contact details for DPO if there is one and their name subject to opt-in.

Exemptions similar to those under the current notification regime may apply.

Failure to pay a fee or to pay the correct fee, is subject to a maximum penalty of £4,350 (150% of the Tier 3 payment).

Article 29 Working Party GDPR guidance

The WP29 has finalised guidance on breach notification, fines (no changes) and automated decision making and profiling.

It has also published draft Article 49 GDPR for consultation. Article 49 deals with derogations for transfers of personal data to third countries.

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

WhatsApp signs undertaking with ICO

WhatsApp has signed an Undertaking with the UK Information Commissioner's Office committing to not sharing personal data with Facebook until it can do so in compliance with the GDPR.

The Undertaking is the outcome of the ICO's investigation of WhatsApp commenced in August 2016 into whether the company could legally share users' data with Facebook in the manner set out in its updated privacy policy.

ICO investigation into data analytics for political purposes

Following the revelations in the Observer and NY Times of Cambridge Analytica's use of Facebook data, the ICO has stressed that her ongoing investigation into the use of data analytics for political purposes, will look at the circumstances in which Facebook data may have been illegally acquired and used.

Cambridge Analytica is alleged to have obtained Facebook data of between 30-50m users. The data was collected through an app set up by an academic, which asked users to sign up voluntarily, take a personality test and agree to let their data be used for academic use in exchange for a small payment. 270,000 users signed up but were either unaware or agreed to the app harvesting the data of all their Facebook friends, leading to the data of up to 50m users being retained.

The data was then passed to Cambridge Analytica who had funded the data collection, where, according to whistleblower Christopher Wylie, the data was analysed and used to target ads and stories and to create software to predict voter outcome.

Facebook is accused of sharing user data without consent and failing to warn users that Cambridge Analytica had their data, as well as security failings. One former employee has said that Facebook routinely lost control of data sent to external developers while he worked at the company between 2011-12 and failed to conduct effective privacy audits on developers. Facebook says the data was transferred to Cambridge Analytica in breach of its platform policies.

The ICO applied for a warrant to enter Cambridge Analytica's premises and carry out an investigation.

The warrant to inspect the premises of Cambridge Analytica was executed at 20.00 on 23 March 2018.

On 24th March an ICO spokesman stated: "We will now need to assess and consider the evidence before deciding the next steps and coming to any conclusions.

"This is one part of a larger investigation by the ICO into the use of personal data and analytics by political campaigns, parties, social media companies and other commercial actors."