# Data Protection Newsletter

July 2017


## Headlines this month:

- Queen's Speech
- Revised subject access guidance
- Department for Culture Media and Sport consultation on GDPR derogations
- Readiness for GDPR
- Recent data breaches

## Commentary:

## Queen's Speech

**In the Queen's Speech, the government made clear its intention to 'ensure that the United Kingdom retains its world-class regime protecting personal data' through implementation of the General Data Protection Regulation and the EU Enforcement Directive.**

It cements the fact that GDPR will replace the Data Protection Act 1998 on 25th May 2018. The government has highlighted that the new rules will empower individuals to have more control over personal information specifically referencing the Right to be Forgotten.

Background notes to the Queen's Speech highlighted the following benefits:

- Meeting manifesto commitments to provide people new rights to "require social media platforms to delete information held about them at the age of 18" and "bring forward a new data protection law".

- To ensure that the UK data protection framework is suitable for the digital age and place us at the forefront of technological innovation, international data sharing and protection of personal data.

For further information contact Mike Bradford or Helen Lord at Regulatory Strategies
consultancy@regulatorystrategies.co.uk

- To implement the General Data Protection Regulation allowing us to meet our obligations while we remain in the EU and to allow us to be able to continue to share data with EU member states after we leave the EU.

## Revised subject access guidance

**The ICO has published a revised Subject Access Code with a view to encourage organisations not only to comply with legal obligations but to see handling them as an 'opportunity for you to improve your customer service and service delivery'.**

The ICO has stated:

*"We consider it good practice for you to engage with the applicant, having an open conversation about the information they require. This might help you to reduce the costs and effort that you would otherwise incur in searching for the information."*

One significant element of the guidance is that the ICO states that it does not expect organisations to ask staff to search their private emails or personal devices unless there is reason to believe that they are holding relevant personal information.

The ICO also expects organisations to respond to subject access requests (SARs) that are made through any social media sites to which they subscribe.

The ICO also states that it:

*"...would not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously deleted personal data held in electronic form. The Commissioner does not require organisations to expend time and effort reconstituting information that they have deleted as part of their general records management."*

The code states that an organisation taking a positive approach to subject access would have the following indicators in place:

- **Training:** All staff should be trained to recognise a SAR as part of general data protection training and more detailed training should be provided to relevant staff
- **Guidance:** Organisations should have a dedicated data protection page on intranets with links to SAR policies and procedures
- **Request handling staff:** A specific person or team should be responsible for handling requests and more than one member of staff should know how to deal with them
- **Data protection experts:** Large organisations should have data protection experts – the responsibility will fall ultimately with the Data Protection Officer post-GDPR implementation
- **Monitoring compliance:** Compliance with SAR handling should be monitored.

**The code also provides specific guidance to organisations who receive bulk requests recognising that these are often generated by claims management companies.**

## Department for Culture, Media and Sport consultation on GDPR derogations

**The Information Commissioner's Office has published its response to the Department for Culture, Media and Sport's consultation on GDPR derogations.**

The response states:

*"Our general approach is to favour replicating existing arrangements under the DPA where experience shows that they work satisfactorily. This will minimise disruption and bring certainty and coherence to the data protection regulatory regime. We support the introduction of new derogations only where we believe this to be necessary for the effective functioning on GDPR or where there is a clear need"*

Some of the ICO's response is summarised below:

- It proposes that the role of the UK supervisory authority should be fulfilled by the ICO but acknowledges that some current arrangements may require revision.

- The GDPR provides an opportunity to ensure key powers and obligations are extended under national law which, again, may fall out of the scope of current arrangements.

- The ICO should retain the investigatory, authorisation, corrective and advisory powers currently provided for under the current data protection legislation.

- There is a recommendation that fines levied should remain 'proportionate' and the ICO wishes to be able to continue to impose administrative fines rather than those fines to be imposed.

- In relation to criminal convictions, the ICO states that unduly restricting access to such data may allow individuals to censor their histories to present a misleading picture of themselves and thereby facilitate fraud or other unlawful behaviour.

- The ICO favours and approach where even quite young children can access appropriate online services without the consent of a parent or guardian.

## Readiness for GDPR

**A survey conducted by Privacy Laws & Business has shown that less than half of respondents have created a data breach notification process despite notification becoming a mandatory requirement under GDPR. In addition only half of respondents have created a staff training programme despite there being an accountability requirement under GDPR.**

64% of respondents had already appointed a Data Protection Officer and half of respondents were currently undertaking a data protection audit. A quarter of respondents said they had reviewed less than 25% of their data protection policies.

82% had established the purposes for which data is processed but only 14% had reviewed supplier contracts and most organisations had not reviewed their methods for obtaining consent.

## Recent data breaches

### Royal Free NHS Foundation Trust

The ICO has ruled that Royal Free NHS Foundation Trust failed to comply with the Data Protection Act after providing patient details to Google DeepMind. Details of around 1.6 million patients were passed as part of a trial to test an alert, diagnosis and detection system.

Elizabeth Denham, The Information Commission, commented:

*"There's no doubt the huge potential that creative use of data could have on patient care and clinical improvements, but the price of innovation does not need to be the erosion of fundamental privacy rights."*

### Boomerang Video Limited

The ICO has sent out a warning to SMEs after Boomerang Video Limited had failed to take basic steps to protect its website from a cyber attack. The ICO stated that regardless of the size of an organisation, it still needs to take its data protection obligations seriously.

The ICO investigation found that regular penetration testing on its website was not carried out, passwords were insufficiently complex, some information was unencrypted and information was held for longer than necessary.

### Conservative Party call centre

The ICO issued a statement after Channel Four News carried out an undercover investigation on a Conservative Party call centre which stated:

*"The Information Commissioner reminded campaigners from political parties of their obligations around direct marketing at the beginning of the election campaign. Where we find they haven't followed the law we will act.*

*"We will be asking the Conservative Party about the marketing campaigns conducted from this call centre."*

**MyHome Installations Limited**

MyHome Installations Limited has been issued with a £50,000 fine for pursuing people who had opted out of telephone marketing. The ICO received 169 complaints from people who were registered with the Telephone Preference Service.

**Morrisons**

Morrisons supermarket chain has been fined for breaking the law regarding marketing emails. Emails were sent to people who had opted out of receiving marking material. The emails were sent to encourage people to change their marketing preferences