ICO and Enforcement Under the GDPR and the Data Protection Act 2018

Following the Information Commissioners Office (ICO) investigation in to data gathering for political campaigning and its first enforcement issued to a company under the Data Protection Act 2018 (DPA18) and the General Data Protection Regulation (GDPR) to the Canadian company AggregrateIQ, there has been little movement in relation to enforcement notices under the new data regulations until now.

Enforcement 1. Data Subjects and Political advertising

Key Words: Article 5 Fairness of Data Processing, Article 14 Notification to data subjects, Article 89 compatibility of data.

In October 2018 and under the ICO's project 'cyberberg', investigations involved companies such as Cambridge Analytica etc. who used personal data obtained from political organisations to target individuals for political advertising on social media.

AggregrateIQ breached the requirement of Article 5 (1) (a, b, c) of the GDPR in relation to the lawful, fairness and transparency of data being processed, whilst under Article 89 such data shall not be incompatible with its initial purposes.it is worth noting the relevance of Article 6 'the 6 principles of processing' along with Article 14 'notification to inform data subjects' as the data was not used for its intended purposes.

The ICO's intention is very clear, as it used utilised section 155 (1)(b) of the DPA 18 'to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 46, 47 or 100 of the DPA18' what is of interest is the ICO attributed its' intention to use the maximum penalty under the GDPR 4% of global annual turnover or €20m.

Enforcement 2. Biometric Data

Key Words: Article 9 processing of special categories, Article 6 Consent.

In 2017 Her Majesty's Revenue and Customs (HMRC) rolled out its voice recognition service to around 7 million customers. Under the GDPR and the DPA18 voice recordings are considered as biometric data. Since the introduction of the GDPR this is the first enforcement action taken in relation to biometric data, as for the first time, biometric data was specifically identified special category data that requires greater protection. After the investigation, the ICO indicated the HMRC did not have adequate consent from its customers and ordered HMRC, via an enforcement notice, to delete any data it continues to hold without consent, by a specified time period.

The commissioner highlighted the scale of the data collection and that "HMRC collected it in circumstances where there was a significant imbalance of power between the organisation and its customers."

"It did not explain to customers how they could decline to participate in the Voice ID system. It also did not explain that customers would not suffer a detrimental impact if they declined to participate." The automated recording failed to obtain explicit consent as required under Article 6.

It was also discovered that a Data Protection Impact Assessment (DPIA) was not in place before the Voice ID system was launched.

The ICO's intention is very clear, as it used utilised section 155 (1)(b) of the DPA 18 'to comply with a data subject's request to exercise rights under Article 16, 17 or 18 of the GDPR (right to rectification, erasure or restriction on processing) or section 46, 47 or 100 of the DPA18' what is of interest is the ICO attributed its' intention to use the maximum penalty under the GDPR 4% of global annual turnover or €20m.

Enforcement 3. Controller duties - Data Subject Access Request

Key Words: Controller Article 4(7), Section 3(6) and 5 of the DPA18, Article 15 Right of Access, Part 3, Chapter 3 DPA18 Rights of the Data Subject.

Following the enforcement of the GDPR in May 2018, the Metropolitan Police Service (MPS) has received an unpresented amount of requests from the public in relation to information held by the service. The ICO has been working with the Metropolitan Police Service (MPS) to address its large Subject Access Requests backlog. However, in a recent report to us the MPS indicated it had more than 1,100 open requests – with nearly 680 over three months old, this is a cause for concern. The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully. Typical response statistics indicated a rate of 91.5% over the statutory deadline. Such a response rate has raised concerns with the ICO who identify through their enforcement notice, the failing of the MPS in demonstrating obligations in respect to the information rights of the individuals for data being processed. Additionally the MPS are to ensure current and prospective individuals who submit access requests are aware of any delays in operational practice which may affect the data subject's statutory rights.

Furthermore, the ICO have identified that companies may extend the time to respond to a subject access request by a further two months if the request is complex or the company has received a number of requests from the individual. Companies must let the individual know within one month of receiving their request and explain why the extension is necessary.

It is worth remembering, the ICO's view is that it is unlikely to be reasonable to extend the time limit if:

- It is manifestly unfounded or excessive;
- An exemption applies; or
- You are requesting proof of identity before considering the request.