CCG ICO update article

Published 28 September 2018

It's been over three months since the GDPR came into force. Here we look at some of the new case law and updated guidance from the ICO regarding data protection issues under the Regulation.

1. Data Breach Reporting

On 20 July 2018, the ICO held a webinar on how best to deal with Data Breach Reporting. They reminded data controllers and processors to refer back to the definition of "Personal Data Breach" in the GDPR, which states that a breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (emphasis added). Therefore it is not the case that any breach of the legislation will be counted as a personal data breach, nor are failing to respond to a SAR or accidentally sending out direct marketing without the relevant legal basis. However, it does cover both accidental and deliberate breaches of security and does not need to involve loss of data.

The reporting requirements kick in when you (as data controller or processor) become aware of a breach. You are only considered to be "aware" when you are reasonably confident that there has been a breach and you can take a reasonable amount of time to investigate until you are confident that there actually has been a breach before reporting. Not every breach needs to be reported – you will first of all need to carry out a risk assessment, for which you should already have a mechanism in place. This should identify:

a) The type of breach;
b) The nature, sensitivity and volume of the data, in particular whether it includes special categories of data;
c) How easy it is to identify individuals from the data;
d) The severity and longevity of the consequences of the breach;
e) Any special characteristics of the data subject(s) – are they vulnerable, children, etc.?

It is important to remember that the 72 hour time limit for notification lasts for 72 calendar hours rather than business hours and this includes over weekends and bank holidays. Data controllers need to have a system in place that ensures breaches that take place outside of normal business hours are detected and appropriately escalated and investigated. If you have encountered a breach but do not consider it to be a reportable breach, then the GDPR requires you to make a record in any event. The ICO may ask to check your record of breaches so it is important that this is kept up to date and accessible.

It is a requirement to inform data subjects about a breach if it is highly likely to affect their rights and freedoms. However, the ICO urges organisations to avoid "notification fatigue", which can occur when data subjects are notified about every insignificant breach, which may result in notifications being ignored and data subjects not realising when they are at serious risk. It should be remembered that the purpose of notifying the data subject is to help them to take steps to protect themselves from the effects of the breach.

2. Redaction of third party data in responses to Subject Access Requests

Data Controllers often have difficulty in making decisions regarding whether or not to release third party personal data when responding to subject access requests. The recent Court of Appeal decision in the case of DB v GMC should assist with the analysis; whilst this case was decided in relation to the Data Protection Act 1998, there are similar provisions in the Data Protection Act 2018 and therefore the rationale is likely to continue to apply in cases judged under the new law.

In this case, a patient had complained to the GMC about the treatment received from his GP, "DB". The GMC commenced an investigation into the doctor's fitness to practice and instructed an independent expert. The expert's report criticised the GP's care but concluded that most GPs would not have realised that the patient had cancer. The GMC sent a summary version of the report to the patient, who then asked for a full, unredacted copy. The GMC treated his request as a subject access request and considered whether to apply the third party data exemption to withhold the GP's personal data. The GP did not give permission for disclosure but the GMC took the view that, on balance, the Report contained the personal data of the patient and should be disclosed to him. The GP successfully appealed the decision and the High Court held that the GMC had failed to lend adequate weight to the GP's privacy rights or to his express refusal of permission.

The Court of Appeal overturned the High Court's decision, stating that there should no presumption or starting point in favour of non-disclosure of third party data. Instead, the wording of the test in the DPA should be followed, namely; whether it was reasonable in all the circumstances to comply with the subject access request without the consent of the

third party. The rights of both parties are important and should be given equal consideration. Whilst the legislation provides a list of example considerations to take into account, this is a non-exhaustive list and the impact of disclosure and non-disclosure on both the data subject and the third party should be considered and balanced against one another.

However, where the data controller reached an equilibrium after taking all considerations into account and did not consider that the balance fell in favour of either disclosure or non-disclosure, at that point the presumption to be applied would be in favour or withholding disclosure, because if there is a precise balance of interests then the controller cannot positively say that it is reasonable to comply with the request without the consent of the third party.

3. Enforcement

Many organisations were concerned that there would be a large increase in enforcement action by the ICO once the GDPR is in force. That fear has not materialised, and as yet the ICO has not taken any enforcement action under the GDPR. However some recent action taken under the DPA 1998 and PECR 2015 gives an indication of the sort of issues they are currently focussing on. For example:

i. London Borough of Lewisham: the ICO issued an enforcement notice after it received complaints regarding the length of time it was taking the local authority data controller to respond to SARs. The ICO found that the data controller had contravened the sixth data protection principle and that its internal systems, procedures and policies for dealing with subject access requests were unlikely to achieve compliance with the provisions of the DPA. There was a backlog of 113 requests, the oldest of which dated back to 2013. The data controller's recovery plan involved eliminating the backlog by 31 July 2018, however an update was provided to the ICO on 25 July explaining that the deadline would not be met.

The Commissioner took the view that "damage or distress is likely as a result of complainants being denied the opportunity of properly understanding what personal data may be being processed about them by the data controller; furthermore they are unable to effectively exercise the various other rights statutorily afforded to a data subject in respect of that data". The Commissioner required that the local authority will fulfil the subject access requests made by data subjects before 25 May 2018 by 15 October 2018. The Commissioner also required weekly progress updates and reminded the LA that failure to comply with the Notice is a criminal offence.

ii. Everything DM Ltd: between May 2016 and May 2017 the firm used its direct marketing system called "Touchpoint" to send direct marketing emails on behalf of its clients for a fee. The ICO found that 1.42 million of those emails were sent without consent. Everything DM Ltd was fined £60,000 for serious contravention of Regulation 22 of the Privacy and Electronic Communications Regulations.

iii. Emma's Diary: a data broking company, which provides advice on pregnancy and childcare, sold personal data to Experian Marketing Services for use by the Labour Party in profiling new mums in the lead up to the 2017 General Election. The data was then used by the Labour Party to target new mums in marginal seats about its intention to protect Sure Start Children's centres. The ICO found that this use of personal data without informing data subjects that their data would be used for political marketing was a breach of the Data Protection Act 1998 and the company was fined £140,000.

Authors

Darryn Hale
London - Walbrook
+44 (0)20 7894 6125
dahale@dacbeachcroft.com

Fiona Gill
London - Walbrook
+44 (0)20 7894 6410
fgill@dacbeachcroft.com