Client Alert: London Borough of Newham fined for Data Security Breach

Date : April 22, 2019

On 4 April 2019 the UK Data Protection Regulator, the Information Commissioner's Office (ICO) fined the London Borough of Newham £145,000 for a data breach involving the data of more than 200 people. Whilst the fine is under the pre-GDPR regime, it has some good pointers on how DPAs will look at an organisation's security obligations under GDPR. There are some technical terms in this note which are explained at www.bit.ly/gdprwords

What happened?

The case involves a detailed set of data on gang members in London and their gang affiliation which was prepared by the Commissioner of Police of the Metropolis and the Metropolitan Police Service (the Met). The Met shared this information with Newham as they were part of a group of organisations trying to reduce gang crime. The Met, Newham and various other authorities were data controllers for this data, known as the Gangs Matrix. The Met produced a redacted and unredacted version of the Matrix.

On 26 January 2017 the Met sent out redacted and unredacted updated versions of the Gangs Matrix with the personal data of 203 data subjects in the Matrix. About 80 of those had a Matrix score of zero indicating that they were no longer a member of a gang, had no further involvement with gang crime or were simply a victim of gang crime.

On 16 May 2017, a gang member told their Probation Officer that they had a snapchat photograph of the Gangs Matrix.

On 20 September 2017, someone associated with a rival gang also told their Probation Officer that they had photographs of the Matrix and the Met were able to establish from that that it was the January 2017 version of the Matrix.

Why did this matter?

The breach could have had serious consequences. Since the data breach, there have been a number of incidents of gang violence including murder, where the victims had appeared on the compromised pages of the unredacted database.

In August 2018 a local safeguarding board concluded its serious case review into the murder of one gang member who had been shot and killed on 4 September 2017. His name had appeared on the Gangs Matrix. The Information Commissioner said that she did not draw a connection between the data breach and the murder but she said this was relevant to the nature and extent of the harm that could result if personal data of the type contained in the unredacted data base was not processed in accordance with the law.

What did the ICO do?

The ICO fined Newham £145,000. This is against the then maximum fine of £500,000.

What are the lessons to be learned?

There are a number of lessons to be learned from this:

1. The ICO was clear that data breaches require a robust investigation. In this case the ICO was critical of Newham who seemed to have had a somewhat cursory internal investigation.
2. Possibly because their investigation was not thorough, Newham were inconsistent in their responses to the ICO. As we have said in earlier alerts (for example our Alert on Cambridge Analytica here

http://www.corderycompliance.com/ico-secures-criminal-convictions-against-ca-in-sar-case/) it is important to treat regulators well. In this case inconsistent emails were sent to the ICO with typographical errors and a general lack of care both on content and form. The ICO said that the fact that the same employee had given two different accounts to the ICO was explained by Newham by saying "*our wording was somewhat ambiguous*". The ICO said "*that is no explanation at all. Newham's earlier wording was not ambiguous. Rather, it provided inaccurate and incomplete information to the Commissioner in the course of her investigation*".

3. Newham were criticised for having no written policy or guidance concerning sharing of the Matrix data bases.
4. Newham were confused as to who was the Data Controller and the Data Processor. In any event they failed to have proper written agreements in place with those third parties.
5. Newham had no systems in place for secure encrypted distribution to all of the recipients of the Matrix.
6. Newham tried to argue that the fine should reduced because of steps that they had taken. The Commissioner said that their non-compliance was so grave that this did not count. She said "*compliance with the law is the bare minimum to be expected. Nor is the fact that the incident was a single identified incidence of sharing of the unredacted data base; that is an inherent part of the breach and if a single incident is sufficiently serious to warrant a monetary penalty it cannot alter or operate as a mitigating factor* ".
7. Newham did not notify the ICO quickly enough when gang members revealed that they had unauthorised access. The ICO emphasised that, even under the old law, the ICO should be told promptly. GDPR has since introduced specific reporting obligations which will mean that most breaches have to be reported within 72 hours. There is more detail on this in our GDPR FAQs at www.bit.ly/gdprfaq. The ICO said that it was irrelevant whether or not Newham believed that others, including the Met, were letting the ICO know. As a Data Controller it was their responsibility to report the breach.
8. The ICO also criticised Newham for not undertaking a Data Protection Impact Assessment (DPIA). Again, DPIAs were voluntary pre-GDPR but compulsory in cases like this after.

There is more information on handling data breaches here http://www.corderycompliance.com/dealing-with-a-data-breach/

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.