Risk control

Newham Data Breach 2019

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

25 YEARS OF DEDICATION IN ACTION

When Data Sharing Goes Wrong…

Introduction

In April 2019, the Information Commissioners Office (ICO) fined the London Borough of Newham £145,000 for the wrongful disclosure of the personal information of more than 200 people who featured on the Police intelligence database – the Gangs Matrix.

The Gangs Matrix is a database that holds information of alleged gang members. The council, police and other statutory partners use the matrix to support their work in preventing and detecting crime, deterring gang activity and offering support for vulnerable children and young people.

The Information Commissioner has issued an enforcement notice to the Metropolitan Police Service in a bid to drive them to make changes to the matrix in order to ensure it complies with data protection laws.

Circumstances of the Breach

The Gangs Matrix had been sent to Newham Council by the Metropolitan Police Service as they were partners working together and with others to tackle gang violence in the Borough. In January 2017, a council employee sent an email to 44 recipients which included the council's own Youth Offending Team as well as external organisations. That email contained both redacted and unredacted versions of the Gangs Matrix.

As a result, information pertaining to 203 individuals was shared. The information included dates of birth, home addresses, names of their alleged associated gangs and whether they were knife carriers or prolific firearms offenders.

Breaches can have Consequences

In 2017, after the breach, the London Borough of Newham experienced a spike in gang related violence with victims including people who featured on the shared Gangs Matrix. The ICO investigation found that after the breach, rival gang members had obtained and shared via social media – photographs of the unredacted information from the Gangs Matrix. That same year, a 14 year old boy who was named in the released information died and the Mayor of Newham has apologised personally to the mother of the boy for the *'profoundly regretful data breach*[1]*'*.

The ICO investigation concluded that there was no evidence to show that the breach directly resulted in the increased gang violence activity experienced in the borough, but equally no evidence to show that it did not.

The Findings of the ICO Investigation

The investigation found:

- There was no need for an unredacted version to be shared between such a large number of people when a redacted version was readily available.
- The council failed to report the breach to the ICO after becoming aware of it.
- The breach occurred in January 2017 but the council failed to commence their own internal investigation until December 2017.
- The council did not have any specific sharing agreements, policy or guidance in place to determine how to appropriately handle the data and use the matrix securely.

James Dipple-Johnstone, the Deputy Commission from the ICO said[2]:

"Data protection is not a barrier for information sharing but it needs to be compliant with the law. One of the ways in doing this is by conducting data protection assessments. We have a data sharing code which provides guidance on how to share data safely and proportionately, and we will soon be publishing an updated code".

The Data Sharing Code

The Information Commissioners Office is currently reviewing and updating this Code[3] following the change of the Data Protection Act 2018 becoming law. It is comprehensive and still very much a valid and useful resource tool for organisations to follow in its current state. The final code is expected to be released by the ICO in the autumn 2019.

[1] https://www.newham.gov.uk/Pages/News/Newham-Council-response-to-Penalty-Notice-from-Information-Commissioners-Office.aspx

[2] https://gdpr.report/news/2019/04/05/london-council-fined-by-the-ico-for-gang-members-data-breach/

[3] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

The introduction of the General Data Protection Regulation (GDPR) has increased the compliance obligations in relation to how personal data is shared. When you set this against the background that local authorities are working in partnership with other bodies to deliver their services now more than ever before it highlights a complex working environment fraught with risk and challenge.

Lessons to be learned

In response to the investigation; Newham Council has made changes to its management and processing of personal data which includes reviewing procedures and data sharing agreements, carrying out data impact risk assessments, using secure mail, mandatory training and an independent compliance audit.

These are all positive steps to take and the key message for your own organisation is to ensure your own procedures are robust enough to catch such an error through your current control framework. If not, it is worth seeking independent advice to understand how you can strengthen your own arrangements and tighten your data control mechanisms.

Minimising the Risk of a Breach

Practical steps that can be taken include:

— Being vigilant

— Effective and tested business continuity plan

— Classification of data in accordance with sensitivity

— Software management

— Employee training and awareness

— Drive forward a culture of security.

Summary

Newham Council publicly apologised via its website following the outcome of the investigation and reaffirmed their commitment to protecting their young people. They accepted the gravity of the breach and laid out assurances that they would learn lessons and change practice and protocol to ensure data is protected, shared and stored correctly.

Despite positive conscious action to manage data effectively, there is always the possibility that a breach can occur. More often than not this is due to human error rather than an inadequate process. How you respond to this situation is of paramount importance. Acting quickly, reporting to the ICO and advising all individuals affected by the breach, investigating without delay and implementing urgent corrections to prevent reoccurrence are all key in effectively taking control back of the situation.

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP946-2019