Published on *The National Law Review* https://natlawreview.com

Data Breaches and Spreadsheets: How to Avoid Fines When Excelling

Article By:

Victoria Leigh

The ICO has fined the Police Service of Northern Ireland ("PSNI") £750,000 in what it has described as the "*most significant data breach that has ever occurred in the history of UK policing*"[1]. The ICO imposed the largest ever fine on a public body following the unauthorised disclosure of an Excel spreadsheet containing the personal data of 9,483 police officers and staff. Given the ICO's stated policy for public authorities is for enforcement to act as a deterrent and to remedy data breaches through reprimands and enforcement notices, with the use of fines reserved for the most egregious cases, it is, at first glance at least, surprising to see the level of fine imposed. The fine comes with a word of warning to private sector data controllers that they would not have benefited from the reduction afforded to public sector enforcement and could have faced a fine of up to £17.5 million.

Background

On 3 August 2023, the PSNI received two Freedom of Information (FOI) requests from the website WhatDoTheyKnow (WDTK) requesting details of the number of officers and staff at each rank or grade. This data was compiled by the PSNI's Workforce Planning Team by downloading and editing existing HR Excel spreadsheets. After preparation, the responsive spreadsheet was sent to the Head of the Workforce Planning Team for quality assurance checks. Once reviewed, it was forwarded to the FOI Decision Maker, who chose to disclose the Excel file in its original format rather than convert it to a Word document, due to technical issues.

Unfortunately, the Workforce Planning Team, the Head of the Workforce Planning Team, and the FOI Decision Maker failed to notice that the Excel file contained a hidden tab, and only inspected the visible tab. The hidden tab included personal data for all officers and staff who were in position, suspended, or on a career break at the time of download. This data included surnames and first initials, job roles, rank/grade, PSNI service/staff numbers, location of post, contract type, and gender.

When the FOI Decision Maker uploaded the Excel file onto the WDTK website, this sensitive data was still accessible. The PSNI was alerted to the breach by its officers the same day. The file was hidden from public view by WDTK and deleted from the website shortly after. The PSNI reported the breach to the Information Commissioner's Office (ICO) later that same day.

The political and policing environment in Northern Ireland renders the PSNI personal data especially

sensitive, often with officers concealing their occupation from friends and family. The risk to PSNI members is significant; for example, in February 2023, a senior police officer was shot in Northern Ireland. The data breach significantly escalated risks for PSNI officers, especially for those in covert roles. The PSNI confirmed they were working on the assumption the file had fallen into the hands of dissident republicans, who would likely exploit it to instil fear and intimidation.

Risks and Damages

The ICO found that the PSNI infringed UK GDPR:

1. Article 5(1)(f) by failing to ensure appropriate security of the personal data;
2. Article 32(1) by failing to implement appropriate technical and organisational measures to ensure appropriate security relevant to the risk of processing the data; and
3. Article 32(2) by failing to appropriately assess the level of security required.

The PSNI had failed to use appropriate technical organisational measures to ensure the appropriate security of the data subject. The ICO identified that the data subjects were at risk of psychological harm, severe injury and even death because of the data breach.

Individual accounts of the impact of the breach were instructive in the ICO's evaluation of the gravity of the infringements on the psychological harm caused. Some examples include:

"*I am struggling to sleep and find myself awake at night checking cameras. I have not visited my family home since the spreadsheet data was released as I believe it would put them in further danger.*"

"*Everything has culminated and become too much for me to the point that I have accepted another job outside the police. I am essentially taking a pay cut…not to mention leaving the job I dreamed of since I was a small child and geared my whole life towards."*

"I have quite a unique surname which had been shared in the data breach, I feel that this not only puts my name in the hands of individuals who may seek to do harm but also affects my own personal family as well and my wider family…The PSNI recently had a senior Officer shot so the threat does feel very real."

Penalty Assessment

The ICO, under UK GDPR, must ensure penalties are effective, proportionate, and dissuasive. The penalty level is determined by factors such as the nature, gravity, and duration of the infringement, whether it was intentional or negligent, actions taken to mitigate damage, and the controller or processor's responsibility.

A breach of integrity and confidentiality can result in fines up to £17.5 million or 4% of the total worldwide annual turnover, whichever is higher. In this case, the seriousness was heightened due to the greater risk to PSNI officers/staff, the regular nature of the data processing, and the damage suffered. The ICO found the infringements were negligent and that PSNI should have known the risks. This warranted a penalty.

Calculating the penalty

The ICO follows fining guidance which sets out a five-step approach to the penalty. Considering the fixed statutory maximum amount, the seriousness and the turnover the ICO found the starting point to be £5.6 million. There were no aggravating or mitigating factors, and a penalty of this size would satisfy the requirement of being effective and dissuasive. However, as the ICO's approach to public sector enforcement is to use fines only in the most egregious cases given that the impact of a public sector fine is often felt by the victims of the breach in the form of reduced budgets for vital services, the penalty was reduced to £750,000. A stark warning for those organisations outside of the public sector which wouldn't benefit from the same reduction.

Key Takeaways

The PSNI's failure to implement appropriate technical and organisational measures was found to be an important factor in determining the penalty imposed in this case. This therefore demonstrates the importance of having appropriate (and effective) technical and organisational measures for data practices in place, not only to mitigate the damage suffered by data subjects but also so that they can be used as a mitigating factor to reduce the level of any fine.

Training

Organisations must appropriately train staff who are involved in processing data to ensure that they recognise the risks associated with hidden tabs in spreadsheets. In October 2024, Southend-on-Sea Council received a reprimand after hidden personal data in a spreadsheet was unintentionally included in response to a FOI request. The ICO emphasised the importance of training staff on the various Excel tools, particularly the "*Inspect Document*" feature.

In 2018, the Royal Borough of Kensington and Chelsea was fined £120,000 for failing to provide any (or any adequate) training to the FOI team regarding the functionalities of Excel spreadsheets. Similarly, in 2016, Blackpool Teaching Hospitals NHS Foundation Trust received a £185,000 fine for not adequately training the web services team on Excel functions and for not providing guidance to the team to check spreadsheets for hidden data before uploading them to its website.

Check

Another key takeaway is to thoroughly check documents that are being uploaded to public systems as, despite passing through three different workforce streams, the PSNI failed to detect the hidden tabs. The finding by the ICO that the PSNI was negligent included the fact that the PSNI ought to have known that spreadsheet files are prone to hidden data and, therefore, human error. To overcome this, data controllers should ensure that they are diligent and take due care when checking what documents are being submitted in response to FOI, DSAR or other information requests or pursuant to contractual obligations.

Act Fast

This case also shows the importance of acting quickly if an organisation experiences a data breach. The PSNI requested the removal of the data from WDTK 37 minutes after becoming aware of the breach. Although this was a prompt response, the ICO did not consider the removal from the website to amount to a mitigating factor as it was an action in line with what would reasonably be expected of a police force responding to a severe data breach.

Guidance The ICO has issued an advisory notice with recommendations to ensure personal

information is not disclosed in response to information requests. Further guidance has been published including "*how to disclose information safely*"[2], and a checklist for public authorities[3] to use for the safe and appropriate disclosure of information. This guidance is relevant and helpful for all organisations, not just public authorities, and sets out key considerations when disclosing information including the use of Excel, converting the data format, publishing data and ensuring appropriate managerial sign off.

---

[1] PSNI Independent review final report, 11 December 2023, p.2-3.

[2] How to disclose information safely

[3] disclosure-checklist-v1_0.docx

National Law Review, Volume XIV, Number 323