Revenue Service reprimanded following breach of financial information

The Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law')
Public Statement
Issued: 11am 16 December 2024
Controller: The Revenue Service

What happened?

Following a data breach where personal information was erroneously sent to an incorrect email address the Data Protection Authority has found that the Revenue Service failed to ensure that appropriate security safeguards were in place. This breach involved the personal information of people who owed money to the Committee for Health & Social Care.

The Revenue Service's policy at the time of the breach was that emails containing personal data should be sent using a specialised secure platform. Further, to help employees comply with this policy, the Revenue Service had implemented an enhanced version of the platform which displayed a pop-up when sending e-mails to external parties, requiring the user to select whether the platform be used. In this case neither was the policy followed, nor the enhanced version installed.

This was not the first time that Revenue Service has reported a breach of this sort to the Authority. In 2022, the Revenue Service notified the Authority of a personal data breach following an e-mail being sent erroneously to an unintended recipient.

Following this breach, the Revenue Service discovered that not all employee accounts were configured with the enhanced version and committed to take further steps to ensure that this was done going forwards. Despite this, in this instance the enhanced version had not been installed.

The Inquiry also found that there were several other breaches where the Revenue Service had failed to send e-mails in line with this policy.

Why was that a problem?

When processing personal data, organisations must take reasonable steps to ensure an appropriate level of security.

Due to the sensitive nature of personal data processed by the Revenue Service, it was reasonable for e-mails to be sent using the specialised secure platform. Amongst other benefits, this platform allowed for access to email content to be controlled and revoked. Had

the e-mail been sent using this platform, the unintended recipient's access could have been immediately revoked, upon notification that it had been sent to the incorrect e-mail address.

Had the Revenue Service acted upon what was revealed from earlier breaches, that some staff were failing to comply with this policy, there would have been additional measures in place to mitigate the impact of this personal data breach.

What has happened as a result?

The Authority has issued a reprimand against the Revenue Service in relation to this breach.

We are pleased that the Revenue Service has since implemented robust measures to ensure that the enhanced version is installed on employee computers and that the policy of sending e-mails using the specialised secure platform is respected and followed.

What can be learned from this?

While the Revenue Service had previously taken several steps towards ensuring the security of personal data, security safeguards against breaches are a dynamic rather than static responsibility. It is not sufficient to just have policies and procedures in place, they must be followed, monitored and updated as new security risks are revealed. This is especially relevant in the digital era where technological risks are a persistent and continuously evolving reality.

Additionally, while organisational measures such as policies can be effective tools to improve an organisation's security posture, technical measures must also be considered to support adherence to the policies and minimise security failings due to human error. This is particularly important where there is evidence that policy is not being followed.

This matter also highlights the importance of ascertaining the effectiveness of security measures in response to breaches to identify whether further steps should be taken.

Technical Background

1. This is a public statement made by the Data Protection Authority ('the Authority') under section 64 of The Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law').

2. In this case, the Controller is the Director of the Revenue Service ('the Revenue Service').

3. Section 69 of the Law allows the Authority to conduct an inquiry on its own initiative into the application of the Law, including into whether a controller or processor has breached or

is likely to breach an operative provision under. In this case, the Authority opened an Inquiry after receiving notification from the Revenue Service of a personal data breach under section 42 of the Law.

4. Section 41 of the Law requires that controllers and processors take reasonable steps to ensure a level of security appropriate to the personal data.

5. Additionally, the principle of integrity and confidentiality within section 6 of the Law requires that personal data is processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. The Authority has determined that the Revenue Service breached sections 6 and 41 of the Law for the following reasons:

- Revenue Service policy at the time of the breach was that all e-mails containing personal data be sent using a specialised secure platform.

- To assist employees in complying with this policy, the Revenue Service implemented an enhanced version of the specialised secure platform that displayed a pop-up when sending e-mails to external parties, requiring the user to select whether the e-mail should be sent using the platform or not.

- Following a breach in July 2022, the Revenue Service identified that some employee accounts did not have the enhanced version of the specialised secure platform configured. However, despite a commitment to ensure this was done in future, at the time of the breach this enhanced version of the specialised secure platform was not configured on the sending employee's account.

- As the employee was aware of the error at the time of sending the e-mail, the use of the specialised secure platform would have allowed them to immediately revoke access to the content and review the audit log to establish whether the e-mail had been accessed by the erroneous recipient.

- There were also signs within breaches logged internally between July 2022 and April 2024 suggesting that employees were not using the specialised secure platform in line with policy.

- These signs should have indicated a requirement to establish why some employees were not using the specialised secure platform, including whether the relevant employees had the enhanced version the platform installed.

- These signs also indicated that policy alone was proving insufficient to ensure that e-mails were sent using the specialised secure platform, meaning that measures to reduce the reliance upon human intervention should have been considered. Measures to automatically send all e-mails containing attachments using the specialised secure platform have now been implemented by the Revenue Service.

7. Section 73 of the Law sets out the sanctions that are available to the Authority where a breach determination has been made.

8. A Reprimand has been imposed against the Revenue Service in respect of its breaches of sections 6 and 41 of the Law.

9. Section 84 of the Law provides for an appeal by a controller or processor to the Court against a determination made by the Authority. Any such appeal must be made within 28 days of the issuance of the determination.