Reprimand issued to Beauvoir Limited regarding steps to protect outgoing mail

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Law")
Public Statement
Issued: 2pm 20 January 2025
Controller: Beauvoir Limited ("Beauvoir")

What happened?

In order for their pension fund to be cashed in, an individual sent Beauvoir a set of sensitive, notarised ID/financial documentation including:

- Signed and countersigned copies of their passport
- Property details
- Their last tax return
- The front page of their bank book, detailing financial information such as their IBAN
- Details of the individual's savings and net worth
- Their residency card, detailing their tax number and health card number
- A utility bill and last property tax bill

To facilitate this process, Beauvoir sent these documents by ordinary mail to a third-party organisation. However, they were subsequently informed by the intended recipient that the documents had not arrived. As no additional measures had been implemented to monitor outgoing post in transit, such as tracking or recorded delivery, Beauvoir were unable to determine the location and/or status of the documents. Subsequent enquiries with the third-party to establish the fate of the documents meant the individual was only informed of the loss of their documents one month later. During this period, no formal breach report was submitted to the Data Protection Authority ("the Authority").

As a result, the individual submitted a formal complaint to the Authority, raising concerns regarding Beauvoir's handling of their personal data.

The Law requires that a controller or processor take reasonable steps to ensure a level of security appropriate to the personal data and that these steps take into account:

- The nature, scope, context and purpose of the processing
- The likelihood and severity of risks posed to the significant interests of data subjects, if the personal data is not secure
- Best practices in technical measures and organisational measures
- The costs of implementing appropriate measures

The Authority's investigation found that Beauvoir did not have a policy in place regarding outgoing mail and therefore insufficient measures were implemented, considering the sensitivity of the documents sent.

Why was that a problem?

Ordinary mail is not an appropriate or proportionate form of transmission for sending important and sensitive personal information by post. Tracking facilities for outgoing mail allow the sender to monitor the progress of post in transit and identify when it has arrived at its destination or otherwise been unsuccessful. Requiring a signature, indicating receipt, ensures there is a record that both parties can refer to when determining what has occurred.

Due to Beauvoir's lack of policy surrounding outgoing mail, these documents were sent with an inappropriate level of security and ultimately led to confusion as to the fate of the personal data in question. This created stress and frustration for the data subject, who had entrusted Beauvoir with their sensitive personal data and was now potentially at risk from external bad actors, who may be in receipt of the notarised documentation and choose to target the individual for fraudulent purposes.

This case was further exacerbated by the delay in identifying the issue and notifying the individual of the loss of their data, leading to a protracted period where they were unable to take any steps to mitigate any risk to themselves.

What has happened as a result?

Following the Authority's Inquiry, Beauvoir were found to have breached the Law by failing to take reasonable steps to ensure the security of personal data, with the Authority issuing a reprimand to Beauvoir.

Beauvoir have informed the Authority that they have since updated their procedures to include an outgoing mail policy, requiring that all client data/due diligence documents are sent via recorded delivery/courier moving forward. The Authority commends Beauvoir for taking these remedial actions.

What can be learned from this?

It is important that controllers understand the risks associated with sensitive personal data, including the information contained within identification and similar sensitive documentation, implementing protective measures proportionate to the value of this data and the potential impact mishandling could cause to the relevant individuals.

Additionally, controllers must take steps, not only to prevent the loss of personal data, but to ensure they can quickly identify if and when a breach has occurred, to help limit any perceived impact to the affected data subject in a timely manner. Whilst some of these measures, both technical and organisational, may not actually prevent a breach

from occurring, they are nonetheless essential to the controller maintaining compliance with the Law. The absence of these measures can pose a risk to the significant interests of individuals; therefore, controllers should regularly review policies and procedures and patch any potential gaps to protect the personal data they are processing.

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 Beauvoir Limited ("Beauvoir").

3. Where a complaint is made under section 67 of the Law, the Authority can investigate to determine if any operative provisions of the Law have been breached.

4. Section 41(1) of the Law requires that a controller or processor take reasonable steps to ensure a level of security appropriate to the personal data.

5. Section 41(3) of the Law requires that, in discharging the duty in subsection (1), the controller or processor must take into account:
   (a) the nature, scope, context and purpose of the processing;
   (b) the likelihood and severity of risks posed to the significant interest of data subjects, if the personal data is not secure;
   (c) best practices in technical measures, organisational measures and any other steps that may be taken for the purposes of subsection (1); and
   (d) the costs of implementing appropriate measures.

6. The Authority has determined that Beauvoir breached section 41 of the Law by failing to consider the nature of the personal data contained within certain sensitive documents as well as best practices to mitigate the risks posed to that data when being sent by post. As such, they have failed to take reasonable steps to ensure the security of information of this nature.

7. Section 73 of the Law sets out the sanctions that are available to the Authority where a breach determination has been made. In this case, the Authority imposed a reprimand upon Beauvoir.

8. Section 84 of the Law provides for an appeal by a controller to the Court against a determination made by the Authority. Any such appeal must be made within 28 days from the date the controller receives the Authority's determination.