HSC reprimanded for delayed breach notification

The Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law')
Public Statement
Issued: 2pm 4 July 2024
Controller: The Committee for Health and Social Care ('HSC')

This is the fifth public statement issued by the Authority in relation to HSC. HSC is a large organisation with multiple service areas, and this is the first for this particular service area.

What happened?
The Committee for Health and Social Care ('HSC') failed to notify the Data Protection Authority ('the Authority' or the 'ODPA') and affected individuals of a personal data breach within the period required by the Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law').

In December 2023, HSC became aware of a data breach which affected the personal data of three individuals.

The Law requires that all personal data breaches be reported to the Authority except where the breach is unlikely to result in any risk to the significant interests of an individual. This notification must be made within 72 hours, unless it is not practicable to do so.

In this case, HSC failed to notify the Authority until 52 days after becoming aware of the breach.

HSC explained the reason for this delay to be that the matter required further internal investigation to ascertain the extent of the breach, as some elements were under dispute. Despite this, the Authority considered that HSC had sufficient information from the outset to ascertain that there had been a personal data breach, and that there was no valid reason why HSC should not have notified the Authority within 72 hours.

The personal data that was subject to the breach included information relating to substance misuse, with HSC determining that the breach was likely to present a high risk to the significant interests of the three individuals that it affected. Where this is the case, individuals must be given written notice of the breach as soon as practicable.

HSC failed to notify these individuals until, in one case – 50 days, and in the other two cases – 62 days, after becoming aware of the breach.

HSC explained that it had needed to take steps to verify the accuracy of contact details it held for two of these individuals, prior to sending written notification. While this was a reasonable step to take, HSC failed to do this in a timely manner, waiting until it had notified

the Authority of the breach and not as soon as practicable as required by the Law.

Why was that a problem?
The purpose of notifying the Authority of personal data breaches is to demonstrate accountability under the Law, allowing the Authority to ensure that appropriate steps are taken to address the breach. Further, given the Authority's expertise in breach management, early engagement with the Authority can help to mitigate damages from any given breach.

The failure to notify the Authority within the period required by the Law meant that the Authority was unable to ensure that appropriate steps had been taken by the Controller until a significant time after the breach had occurred.
The requirement to notify individuals where a personal data breach is deemed likely to result in a high risk to significant interests allows individuals to understand what has happened to their personal data and to take any precaution that they consider necessary to protect their interests. The failure to notify individuals as soon as practicable meant that there was a protracted period where these individuals were unable to take any steps to protect their significant interests.

What has happened as a result?
Following the Authority's Inquiry, HSC were found to have breached the Law by failing to notify the Authority and individuals within the time periods required by the Law, with the Authority issuing a reprimand to HSC.

What can be learned from this?
It is important that controllers notify the Authority of personal data breaches as soon as practicable.

Where a controller cannot provide all information that is required to be given within the 72 hours, it can be provided in stages. However, the initial report must still be made within that 72-hour period.

It is also vital to ensure that sufficient information is given to individuals in a timely manner to allow them to take any steps they consider necessary to protect their interests.

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 Committee for Health and Social Care ('HSC').
3. The Authority may conduct an Inquiry under section 69 of the Law on any basis, into whether a controller or processor has breached or is likely to breach an operative provision

of the Law. In this case, the Authority had concerns in respect of the length of time taken by HSC to notify the Authority and data subjects of the breach.

4. Section 42(2) of the Law requires that where a controller becomes aware of a personal data breach, it must give the Authority written notice of it as soon as practicable, and in any event no later than 72 hours after becoming aware of it, unless this is not practicable.

5. Section 43(1) of the Law requires that where a controller becomes aware of a personal data breach that is likely to pose a high risk to the significant interests of a data subject, the controller must give the data subject written notice of the breach as soon as practicable.

6. The Authority has determined that HSC breached sections 42 and 43 of the Law by failing to notify the Authority and affected individuals of the breach as soon as practicable.

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 HSC.

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 which in this case ends on 29 July 2024.