Enforcement order issued to The Committee for Health and Social Care over data protection training and governance

The Data Protection (Bailiwick of Guernsey) Law, 2017 **(the Law)**
Public Statement
Issued: 12pm Thursday 23 February 2023
Controller: The Committee *for* Health and Social Care ('HSC')

What happened?
The Data Protection Authority initiated two independent investigations. Both investigations focused on whether the Committee *for* Health and Social Care's ('HSC') processes for staff training and personal data security, were robust enough. The investigations were launched following concerns brought to the Authority's attention by two complainants. One complaint related to unauthorised access to medical information held on hospital systems, whilst the other complaint related to an HSC staff member using a service-user's device for work purposes.

Both complaints resulted in investigations that were lengthy and complex and involved significant communications with HSC.

The first complaint was about a number of incidents whereby the Complainant's medical record was accessed without apparent justification. The investigation found that training provided to HSC staff members was not robust in either its quality, or the process by which it is rolled out to staff. A number of the staff members who had accessed the medical record in question had not done the requisite training mandated by HSC and the Authority determined that the processes to monitor and enforce the completion of the mandatory training were ineffective.

The second complaint related to HSC staff members use of a service-user's personal device for work purposes, this arose out of poor governance. The investigation determined that one of the primary reasons for the device being used to carry out work, was that the option to utilise a workplace device was not available to the staff members in question. This was, in part, caused by the fact that a member of staff had left HSC's employment without returning the HSC issued laptop that had previously been utilised by the staff members in question.

HSC was unaware that the device was missing at the time due to the leavers process that was in place having not been correctly followed.

The Authority concluded that had a robust process been in place and implemented, this incident may have been avoided entirely. It is understood that workplace devices have since been issued.

In conclusion, the Authority determined that HSC had:
1) failed in their duty to comply with the data protection principles,
2) failed to take steps to ensure compliance with the data protection principles, specifically ensuring that processes regarding staff training and staff leavers policies were robust enough, and
3) failed to take reasonable steps to ensure the security of personal data they were processing.

Why is this a problem?
HSC processes large amounts of very sensitive personal data raising the risk level of any processing and requiring more robust compliance as a result. Having concluded the two investigations, the Authority determined that HSC's governance fell short of expected standards. In both circumstances relevant to these investigations, HSC were unaware of the issues until the Complainants themselves raised their concerns.

What has happened as a result?
The Authority issued an enforcement order to the Committee *for* Health and Social Care to address the identified shortcomings in its data processing practices. This means that HSC will have to demonstrate, by 31 March 2023, that it has improved those processes.

What can be learned?
Process and governance matters. The greater the potential harm, the more robust the process should be. It should be noted that even minor procedural missteps can have significant and sometimes entirely unexpected consequences. It is not enough to react to data protection issues, controllers must be proactive in how they assess and manage risk in their organisations.

Technical statement
1. The Authority conducted two investigations under section 68 of the Law following complaints made in relation to the processing of personal data by The Committee for Health and Social Care ("the Controller"). The first related to allegations of unauthorised access to a medical record and the second to the alleged use of a service user's device for the processing of personal data by the Controller's staff.
2. As a result of the investigations, the Authority determined that the Controller **breached Section 6 of the Law ("Duty to comply with data protection principles")** with specific reference to the part relating to 'Integrity and confidentiality'. This was due to both investigations finding that measures deployed by the Controller were insufficient to appropriately ensure the security of the personal data in question.
3. Further, the Authority determined that the Controller **breached Section 32 of the Law ("Data protection measures by design and default")**. The Authority concluded that the

Controller had not established and implemented suitable and proportionate measures to ensure processing was carried out in compliance with the Law. In the context of the processing in question, those safeguards should have amounted to more robust governance surrounding staff training to ensure all staff undertake suitable training to understand their obligations and what they should not do and the handling of workplace devices, specifically when a staff member is leaving the Controller's employment.

4. In relation to the second complaint, the Authority determined that the Controller **breached Section 41 of the Law ("Duty to take reasonable steps to ensure security")**. Section 41 requires that the measures implemented by the Controller must ensure that the Controller has, and retains, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. By not implementing sufficient measures in the form of governance it was apparent that the Controller was not able to provide such assurances around the use of devices.

5. In accordance with the powers contained in Section 73 of the Law, the Authority has **issued an enforcement order** to the Controller. This requires appropriate improvements in processes to be made by 31 March 2023.

6. The Controller had the right to appeal this sanction but did not do so.

Legal Framework

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. The Authority may conduct an investigation (under section 68 of the Law) upon receipt of a complaint from an individual where the individual considers that a controller or processor has breached or is likely to breach an operative provision of the Law.

3. In this case, the Controller is The Committee *for* Health and Social Care.

4. Section 71 of the Law requires the Authority to determine whether or not there has been a breach of an operative provision of the Law following an investigation.

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

6. Section 84 of the Law provides for an appeal by the Controller to the Court against a determination made by the Authority. Any such appeal must be made within 28 days. The Controller has not made an appeal in this case.