Following ODPA investigation into IT outage, SoG confirms completion of recommendations

The Data Protection (Bailiwick of Guernsey) Law, 2017 ('the Law')
Public Statement
Issued: 11 February at 12pm
Controller: The Policy and Resources Committee

What happened?

In October 2023, the Data Protection Authority ("the Authority") initiated an Inquiry into the Policy & Resources Committee ('P&R'), following a review into several incidents that took down certain States of Guernsey's IT systems between November 2022 – January 2023. These outages meant people were unable to use the systems and access the personal data held on them.

The Authority's Inquiry, as informed by the review, found that P&R had failed to take reasonable steps to maintain the air conditioning system within a data room, leading to its failure. This failure was one of multiple failures involving other technical and monitoring controls, resulting in the loss of IT services.

The Inquiry also found that prior to the incidents, P&R had failed to implement an IT disaster recovery plan as is necessary to be able to effectively respond to critical incidents such as those encountered between November 2022 and January 2023.

For these reasons, the Authority concluded that P&R did not take reasonable steps to ensure the security of personal data.

These findings, which relate to P&R's data protection obligations, align with the findings of the recently released report of the **Scrutiny Management Committee** focussed on the *'Review of the Future Digital Services Contract with Agilisys (Guernsey) Limited'.*

Why was that a problem?

The Data Protection Law requires that organisations take reasonable steps to ensure they have the ability to secure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

The data room services outages would not have occurred had P&R heeded previous warnings regarding the vulnerability of the air conditioning unit at Sir Charles Frossard House.

The lack of regard paid to warnings concerning the air-conditioning system demonstrated that reasonable steps were not taken to ensure there was an ongoing resilience of States of

Guernsey processing systems and services, which resulted in the loss of access to personal data.

During the Inquiry it was also discovered that there was no IT disaster recovery plan in place at the time of the data room service outages.

The purpose of an IT disaster recovery plan is to reduce the downtime, costs, and business impact of incidents by putting effective, standardised processes in place for when those incidents do occur.

It ensures the resilience and continuity of IT services and that if systems go down unexpectedly that they are brought back up again promptly.

The lack of an IT disaster recovery plan during the data room service outages limited the ability to maintain and restore the availability of servers, and therefore the personal data stored thereon.

What has happened as a result?

PWC's 'Major Incident Review' included an action plan containing recommendations which were intended to reduce the risks to mission-critical IT services provided by the States of Guernsey.

During its Inquiry, the Authority required P&R to report on its progress in implementing the action plan's recommendations.

The Authority is pleased that the Policy & Resources Committee has confirmed that all the recommendations in the proposed action plan have now been completed and is encouraged by their commitment to ensuring adequate safeguards on a going forward basis.

Based on this confirmation and commitment, the Authority issued a sanction in the form of a Reprimand.

Had the action plan not been completed, the Authority would have issued P&R with an order requiring them to take the actions identified in that action plan, holding P&R accountable for putting right the problems identified.

As P&R have already provided confirmation that they have implemented all recommendations, the reprimand issued recognises those actions, and accountability for their successful implementation rests with P&R.

What can be learned from this?

This incident demonstrates the importance of organisations identifying and addressing potential risks posed to the security of personal data.

Organisations that do not regularly assess and mitigate their vulnerabilities are more likely to face system failures.

When a risk area is identified that warning should be heeded. Too often incidents occur in areas of known risks that could have been mitigated if swift action had been taken.

Investing in preventive measures is crucial to avoid such disruptions.

Another critical takeaway is the need to prioritise system resilience and recovery. If organisations do not have robust plans to restore data and services quickly after an incident, outages can last longer, causing significant operational and reputational damage.

Organisations should recognise that underinvesting in security often leads to greater costs down the road. Balancing security costs against risk is vital.

Ensuring the confidentiality, integrity, and availability of personal data is not just about avoiding breaches; it is about maintaining operations and protecting all stakeholders.

Security safeguards are a dynamic rather than static responsibility, requiring continuous monitoring, enhancements, training, and vigilance to prevent incidents and system failures.

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 Policy & Resources Committee.

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.

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. The Authority has determined that the Policy & Resources Committee breached section 41 of the Law for the following reasons:

Sub-section 41(2)(b) requires that:

(b) ensuring that the controller or processor has and retains the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

- PWC's 'Major Incident Review' concluded that the failure of the air conditioning system at Sir Charles Frossard House was the root cause of the initial IT outage.
- During the Inquiry, the Policy & Resources Committee did not challenge its liability in relation to the air conditioning failure.

- The Authority assessed that these IT outages would not have occurred had the Controller heeded previous warnings regarding the vulnerability of the air conditioning.
- The lack of regard paid to the clear warning concerning the air-conditioning system demonstrated that reasonable steps were not taken to ensure there was an ongoing resilience of processing systems and services.

Sub-section 41(2)(c) requires that:

c) ensuring that the controller or processor has and retains the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

- The purpose of an IT disaster recovery plan (also known as an IT service continuity plan) is to reduce the downtime, costs, and business impact of incidents by putting effective, standardised processes in place for when those incidents do occur. It ensures the resilience and continuity of IT services.
- Not having an IT disaster recovery plan limited the Policy & Resources Committee's ability to maintain and restore the availability of servers and therefore the personal data stored thereon.
- The extent to which not having an IT disaster recovery plan added to the duration of the outages is unknown. However, it is said with confidence that it was a factor in the duration of the outages.
- Not having an IT disaster recovery plan constitutes a breach of section 41(2)(c) of the Law due to it limiting a controller's ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

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

7. A Reprimand has been imposed against the Policy & Resources Committee in respect of its breaches of section 41 of the Law. Had confirmation not been received that the recommendations within 'Major Incident Report' had been acted on, an order requiring such action would have been issued.

8. 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.