Delta Finance - POLICY: Personal Data Breach

Introduction

A personal data breach, if not addressed appropriately and timeously, could result in physical, material or non-material damage to individuals as well as financial and reputational damage to our organisation. Where we collect, use and retain personal data, every care must be taken to both, protect that personal data and use it in a lawful manner.

Purpose and Scope

The General Data Protection Regulation (GDPR), has a requirement for our organisation to have a suitable data security framework in place. This policy is an essential part of that framework and sets out the procedure to be followed that ensures a consistent and effective response to a security incident. The policy applies to all employees, contractors and other stakeholders who might have access to or be responsible for the collection and processing of personal data.

Definition

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Reporting an incident

Report any discovery of an incident immediately to your most senior manager. Senior management will ensure that they are contactable for emergencies outside our regular hours of operation. Anyone reporting an incident is encouraged to record as much detail as possible. Be aware that failure to report an incident could potentially attract disciplinary action.

Containment and recovery

The first responder will determine if the incident is still occurring and, if so, the steps that will be taken to minimise the effects of the incident. Thereafter, an initial assessment will be done to determine – severity; what can be done to limit damages or recover losses; who may need to be notified in terms of the initial containment; any involvement of law enforcement; and the course of action to be followed.

Investigation and risk assessment

Our breach procedure will, at the very least, determine – the lead investigator; when the investigation must start; how will risks be assessed and treated; the individuals affected, the effect of the incident on them and what they can to minimise impact.

Notification

If an incident has been contained, it may not be necessary to inform the supervisory authority. If we do have to inform the supervisory authority, it must be done within 72 hours of becoming aware of the breach – unless we can explain why it might not be possible to do so within 72 hours.

Be aware that law enforcement may prevent us from informing individuals whose personal data may be affected by the breach. Where we do need to inform individuals, we will do so timeously and in simple but specific language. We will also consider whether it's necessary to inform other stakeholders – insurers, banks, credit card agents, trade unions. We will keep a record of every incident/breach regardless of whether notification was required.

Evaluation and response

Every incident will require a full review of the causes, the effectiveness of the response and the impact on existing systems and/or procedures. Existing controls will be reviewed to determine whether any optimisation is necessary. We will determine whether any training and awareness of incident detection and response may be necessary. As such, regular desktop training exercises are to be encouraged.