



Data Breach Incident Reporting & Management Standard

| | |
|----------------|--------------------------|
| Approved By | Group Chief Risk Officer |
| Document Owner | Group Risk |
| Input Sought | Privacy Compliance |
| Effective Date | 10 May 2024 |

If it may be necessary to disclose this document in part, or in full, to a third party, approval must be obtained from the document owner prior to disclosure.

Version Control

| Date | Version | Updated By | Description |
|----------------|---------|--|--|
| 31 March 2022 | 1.0 | Regina Phua | <ul style="list-style-type: none"> a. Introduction of the handling of data incidents in addition to data breaches. b. Align key actions in Section 4 to that of the PDPC requirements. c. Notification timeline to PDPC and Affected Individuals are defined in Section 4. |
| 6 January 2023 | 1.1 | Livia | Updated that Business Unit/DPO shall work with the Brands & Communications team to draft the notification communication to the affected individuals. |
| 10 May 2024 | 2.0 | Amirul Ashraf / Daniel Heng / Sharon Tan | <p>Editorial changes across the Standard to improve clarity.</p> <ul style="list-style-type: none"> 1. Purpose, Scope and Definition – amendments to purpose of standard and updates to definition. 2. Roles and Responsibilities – updates to existing roles and responsibilities, introduced new roles for Data Owners. 3. Possible Causes of Data Breaches – updates to malicious activities and human/process error sections. 4. Data Breach Management Procedure – updates to section header, definitions and reporting timeline, added new timeline for critical data breaches, added MAS reporting obligation for licensed insurers. 5. Notification of Data Breaches to The Monetary Association of Singapore (MAS) – added based of MAS Notice 127 for notification of data breaches to MAS for licensed insurers. 6. Resources – updates to related resources for reference. 7. Review – removed version control. |

Contents

| | | |
|----|--|----|
| 1. | Purpose, Scope, and Definition | 4 |
| | 1.1 Purpose..... | 4 |
| | 1.2 Scope..... | 4 |
| | 1.3 Definitions | 4 |
| 2. | Roles and Responsibilities..... | 5 |
| 3. | Possible Causes of Data Breaches..... | 7 |
| 4. | Data Breach Incident & Management Procedure | 8 |
| | 4.1 <i>Contain and Assess</i> | 9 |
| | 4.2 <i>Report</i> | 11 |
| | 4.3 <i>Evaluate</i> | 12 |
| 5. | Resources | 13 |
| 6. | Review | 13 |
| | Appendix - Notification of Data Breaches to The Monetary Authority of Singapore ("The Authority") | 14 |

1. Purpose, Scope, and Definition

1.1 Purpose

Data breaches often lead to financial losses and/or loss of customer trust for the company. In addition, individuals whose personal data have been compromised could be at risk of significant harm if they do not take steps to protect themselves.

The purpose of this Standard is to define the processes and expectations for the effective and consistent management of data breach incidents.

1.2 Scope

The scope of this Standard is Group-wide. It applies to all companies in the Singlife Group, their business operations, support functions and employees.

It is recognized that in some countries outside Singapore, local legislation and regulations may prohibit the direct adoption of this Standard in its entirety. In such cases, the senior management of the legal entity must adopt the Standard to the extent permitted by local laws and regulations and notify the Group Chief Risk Officer of any deviations.

1.3 Definitions

| Term | Definition |
|-------------------------------------|--|
| Data | For the purpose of this Standard, 'Data' refers to personal identifiable information as defined by the PDPA <u>and</u> any information that is classified confidential or secret (i.e. critical data) in the company. |
| Data Breach | Any unauthorized access, collection, use, disclosure, copying, modification or disposal of data; and/or the loss of any storage medium or device on which data is stored in circumstances where the unauthorized access, use and disclosure of the data is likely to occur. |
| Data Breach Incident | Occurrence of an actual or suspected data breach. |
| Data Breach Notification Obligation | <p>The prevailing regulatory obligation stipulated under the PDPA for the notification of data breach involving personal data to the PDPC.</p> <p>Singlife must take reasonable steps to assess if a data breach discovered could result in significant harm to individuals and/or are of significant scale. If so, Singlife must notify the PDPC and the affected individuals of the data breach incident as soon as practicable.</p> |

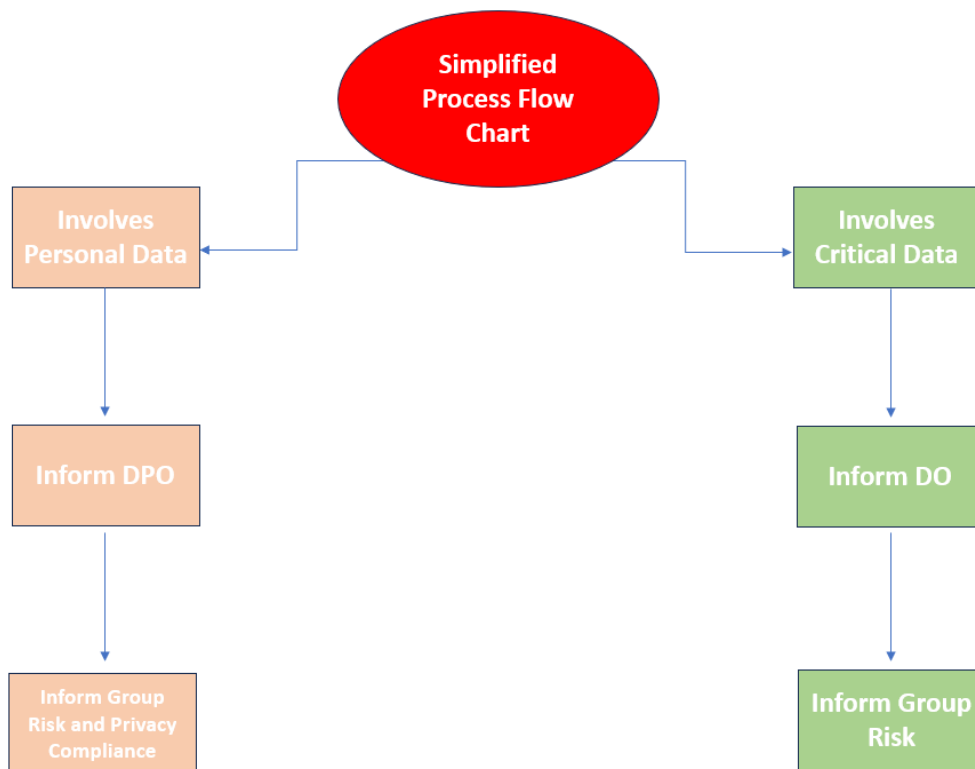
2. Roles and Responsibilities

The roles and responsibilities of various stakeholders for ensuring accountability, ownership and oversight of all data breach Incident is spelt out in the table below:

| Role | Responsibilities |
|---|--|
| Every employee | <p>Without undue delay, any employee who discovered or suspected that a data breach incident has occurred must:</p> <ol style="list-style-type: none"> Escalate the data breach incident to his/her line manager, and <ul style="list-style-type: none"> For breach of personal data, inform the relevant Business/Function Data Protection Officer, or For breach of critical data, inform the relevant Data Owner as soon as they are aware of the incident. Cooperate and provide all evidence and facts pertaining to the data breach incident, Where personal data is breached, work closely with the relevant Business/Function Data Protection Officer to ensure that the data breach incident is effectively managed. This includes containing the damage caused by the data breach incident, implementing mitigating measures to prevent future recurrence, and ensuring that the data breach obligations are followed through till closure, where relevant, Where the breach involves critical data, work closely with the relevant Data Owner to ensure that the data breach incident is effectively managed. This includes containing the damage to the company and implementing measures to prevent future recurrence, and Record/log the data breach incident report in the Singlife GRC System (i.e. Loss Event on MetricStream). <p><i>(The Business Unit where the data breach originated will lead the investigation and remediation activities. This involves determining how many individuals are impacted, the type of critical/personal data involved and whether the data can be retrieved/deleted; identifying the root cause and delivering remediation activities. For example, if the data breach incident was caused by a cyber-attack or IT system lapse, the respective Tech teams will be responsible for leading the investigation and remediation activities, in collaboration with the impacted business functions.)</i></p> |
| Business/Function Data Protection Officer (DPO) | <p>Where a personal data breach is discovered, without undue delay, the relevant Business/Function DPOs must:</p> <ol style="list-style-type: none"> Escalate all actual/suspected data breach incidents to Group Risk and Privacy Compliance (incl. Group DPO), Lead the investigation and manage the incident through to closure, |

| Role | Responsibilities |
|--|--|
| | <ul style="list-style-type: none"> c) Determine the full extent of the incident, establish containment measures, and propose preventive measures, and d) Provide support to Group Risk and Privacy Compliance to prepare/review reports for regulatory notification. e) Prepare and ensure the completeness and accuracy of the Data Breach report. |
| Data Owner | <p>Where a breach of critical data is discovered, the relevant Data Owner must:</p> <ul style="list-style-type: none"> a) Escalate the data breach incidents to Group Risk, b) Lead the investigation and manage the incident through to closure, c) Determine the full extent of the incident, establish containment measures, and propose preventive measures, and d) Prepare and ensure the completeness and accuracy of the Data Breach report. |
| Group Risk (Data Risk Team) | <ul style="list-style-type: none"> a) Provide support on data breach incident management to the DPO or Data Owner, b) Review and ensure completeness and accuracy of the Data Breach report, c) Escalate any significant data breaches that may result in reputational impact to Singlife (such as media reports or negative comments posted in social media) to the Brand, Communication & Marketing team for their handling as appropriate, and d) Seek concurrence from Group Chief Risk Officer or Group Head of Legal, Compliance and Secretariat on data breaches that requires regulatory notification. <p>Where the data breach incident involves breach of personal data, the above responsibilities will be performed in collaboration with the Privacy Compliance Team.</p> |
| Privacy Compliance / Group DPO | <ul style="list-style-type: none"> a) Provide independent assessment to determine whether the personal data breach is notifiable to the PDPC. b) Liaise with PDPC and the Infocomm Media Development Authority (IMDA) on all data breach reporting and follow-ups, if any, and c) Liaise with Regulatory Compliance on the quarterly reporting of non-notifiable data breaches (to PDPC) to the Monetary Authority of Singapore (MAS). |
| Group Chief Risk Officer (CRO) and/or Group Head | <ul style="list-style-type: none"> a) Provide approval on data breaches that requires regulatory notification/reporting, and |

| Role | Responsibilities |
|---|--|
| of Legal & Compliance | b) Escalate any conflicting views on whether the data breaches require regulatory reporting to the Group CEO for final decision. |
| Chief Information Security Officer (CISO) | a) Provide subject matter expert advice regarding data breach incidents that involves cyber security issues, and b) Provide assessment whether reporting of any data breach incident to the Cyber Security Agency of Singapore (CSA) is required. |
| Legal | Provide assessment if reporting to the Police is required. |



Refer to figures 1 and 2 below (section 4) for full timeline and actions required.

3. Possible Causes of Data Breaches

Data breaches could occur for different reasons. Possible drivers (non-exhaustive) that may result in a data breach incident are provided below for guidance:

- a) **Malicious Activities** – This could be perpetrated by an external party or from within the Singlife Group such as:
 - i) Cyber hacking, ransomware, or unauthorized access to databases,
 - ii) Theft of computer notebooks, data storage devices or paper records,

- iii) Scams (e.g. phishing attacks) that trick a staff member into releasing personal data of individuals,
 - iv) Unauthorized access, downloads/printing, or disclosure of data by employees, and
 - v) Unauthorized modification or deletion of data.
- b) **Human Error/Processes** – Most common errors caused by employees are:
 - i) Loss of computer notebooks, data storage devices or paper records containing data,
 - ii) Sending data to a wrong e-mail or residential/mailing address which results in the disclosure of data to a wrong recipient,
 - iii) Improper disposal of data (e.g. hard disk, storage media or paper documents are sold/discarded before all data is properly deleted),
 - iv) Lapses in process and user acceptance tests that have resulted in data related error, and
 - v) Poor cyber hygiene practices such as using weak or poor passwords, resulting in user account being compromised.
- c) **System Deficiency** – This pertains to issues arising from weaknesses of computer hardware or software. For example, errors or bugs in the programming code of websites, databases, applications, internet software downloads and usage of outdated software may be exploited to gain access to personal and critical data stored on computer systems.

4. Data Breach Incident & Management Procedure

To effectively manage data breach incidents, the following actions must be taken:

- a) **Contain** the data breach to prevent further compromise of data and implement mitigating actions to minimize potential harm arising from the incident,
- b) **Assess** the effectiveness of the containment actions by thoroughly reviewing the facts and evidence. Continuous efforts should be made to prevent further harm in the interim, until all remediation actions are completed,
- c) **Report** the data breach incident to the relevant authorities and/or affected individuals, where personal data is involved in compliance with the PDPA, and
- d) **Evaluate** the company's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

Figure 1 and 2 illustrates the timeline and core actions when handling a data breach incident.

Data breach incidents involving personal data

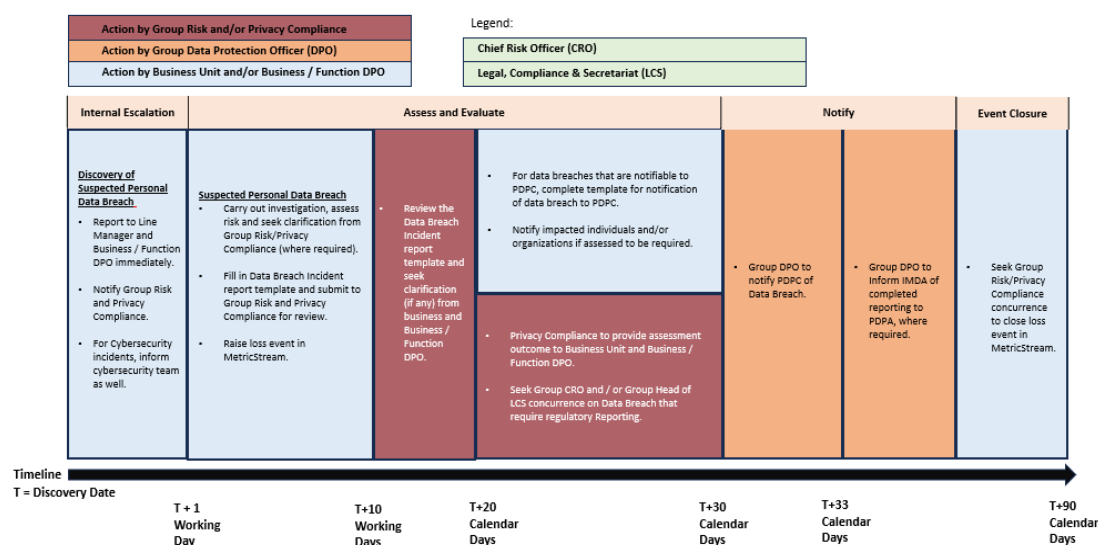


Figure 1: Timeline and Action for Handling Data Breach Incident involving Personal Data

Data breach involving critical data (but not personal data)

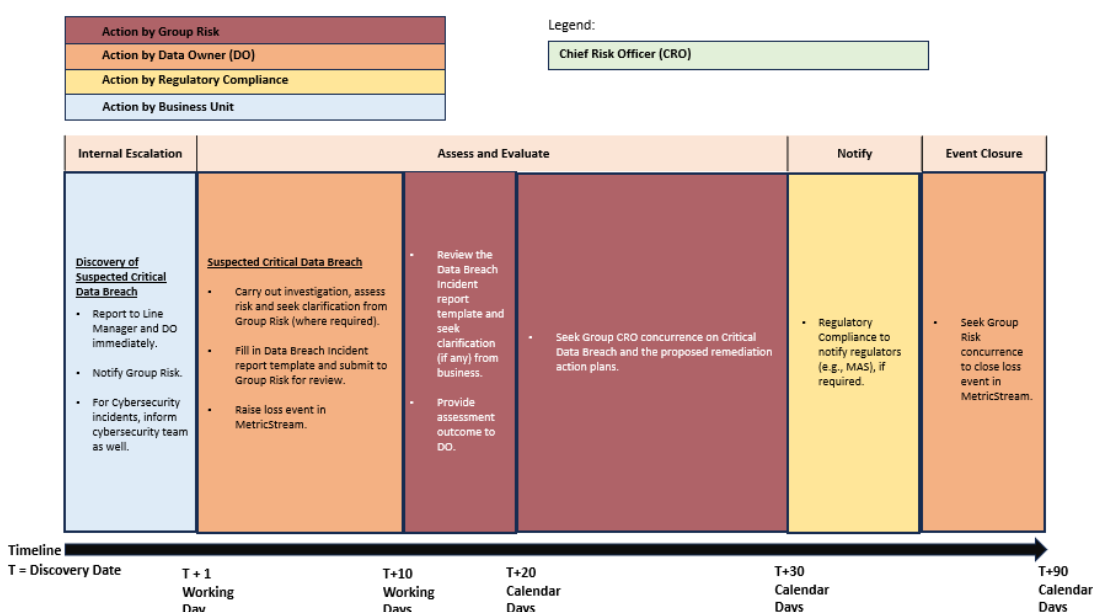


Figure 2: Timeline and Action for Handling Data Breach Incident involving Critical Data

4.1 Contain and Assess

Once a suspected data breach has been reported, an initial assessment should be conducted by the relevant Business Unit together with their DPO to determine the severity of the data breach. The assessment should be done with close consultation from the Group Risk and Privacy Compliance Teams. Where required, Group Risk and Privacy Compliance may notify other internal stakeholders such as Regulatory

Compliance and CISO as well as external stakeholders such as the regulators. The initial assessment should include (but not be limited to) the following information:

- a) What has caused the data breach (i.e. malicious activity, human error, or system error) and whether the breach is still ongoing.
- b) When did the data breach incident occur and when was the breach discovered.
- c) Number of affected individuals.
- d) Classification (i.e. Confidential, Secret) and the type of data fields involved.
- e) Any affected systems, servers, databases, platforms, or services.
- f) Immediate remediation actions taken or will be taken to reduce any harm to affected individual and/or to contain the data breach.

The assessment allows the company to decide on the immediate actions to take to contain the data breach as soon as possible. The breach containment measures will depend on the breach scenario and whether the breach is a paper or electronic breach. Refer to the examples below of possible actions.

a) Compromised System

- i) Shut down the compromised system that led to the data breach.
- ii) Isolate the causes of the data breach in the system.
- iii) Change the access rights to the compromised system.
- iv) Remove external connections to the system.

b) Inappropriate Processes

- i) Stop the practices that led to the data breach. (e.g. shredding paper documents containing personal data instead of throwing into the garbage bin).
- ii) Address lapses in processes that led to the data breach and communicate to all relevant employees.

c) Minimize Loss

Establish whether steps can be taken to recover lost data and limit any damage caused by the breach (e.g. remotely disabling a lost notebook containing personal data of individuals).

d) Compromised Access


- i) Prevent further unauthorized access to the system.
- ii) Reset passwords if accounts and passwords have been compromised.

e) Criminal Activity

- i) Notify Group Internal Audit and the police if criminal activity is suspected and preserve evidence for investigation (e.g. cyber hacking, theft, or unauthorized system access by an employee).
- ii) Notify CSA for cyber-attack incidents.

4.2 Report

The table below sets out the criteria to determine if a data breach is notifiable to the Personal Data Protection Commission (PDPC), Monetary Authority of Singapore (MAS), and Individuals affected by the Data Breach.

| Party | Notification Criteria | Action Required |
|------------------------|---|--|
| PDPC | <p>As part of the PDPA Data Breach Notification (DBN) obligation, organizations, including Singlife, are required to notify PDPC when the data breach:</p> <p>a) results in significant harm to affected individuals (refer to section 20.15 of the appended document on the prescribed classes of data that constitutes significant harm); or</p>  <p>Advisory Guidelines on Key Concepts in th</p> <p>b) it is of a significant scale (i.e. 500 or more individuals are affected).</p> <p>Notify no later than 3 calendar days upon determining that the data breach is notifiable.</p> | <p>Business / Function DPO to complete the template and submit to Group DPO for onward filing on PDPC website.</p> <p>Note: MAS will also be notified via the e-filing on PDPC website</p> |
| MAS | Compliance with MAS Circular No. ID 10/14 which introduced the mandatory data breach notification requirements for licensed insurers in Singapore. | Refer to the appendix |
| Affected Individual(s) | <p>The data breach results in significant harm to affected individuals (refer to section 20.15 in the document attached above under Notification Criteria for PDPC)</p> <p>Notify as soon as practicable, at the same time or after notifying the PDPC.¹</p> | Business Unit/DPO will work with the Brands, Communications & Marketing team to draft the notification ² communication to the affected individuals. |

¹ The timeline to notify affected individuals “at the same or after notifying the PDPC” is spelled out in the PDPC Advisory Guidelines on Key Concepts in the PDPA. While Singlife is not required to obtain PDPC’s clearance on the notification to affected individuals, certain data breaches might warrant PDPC’s further advice before the notification to affected individual is issued.

² Notification to affected individuals should be clear and easily understood; include information such as when the company first became aware that a notifiable data breach as occurred, personal data or classes of personal data that have been compromised, information on any recovery/remedial actions, and contact details of at least one company representative whom the affected individual can contact for further assistance. Where appropriate, parents or guardians of young children whose personal data has been compromised should be notified.

4.3 Evaluate

After all steps have been taken to resolve the data breach incident, the company should review the cause of the data breach and evaluate if existing protection and prevention measures are sufficient to prevent similar breaches from occurring again.

The relevant business unit and DPO may consider the following guidance to identify possible recovery and remediating actions.

a) Operational and Policy Related

- i) Were management control self-assessment (MCA) regularly conducted on both physical and IT-related security measures? Were the action items from the last MCA remediated?
- ii) Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
- iii) Were there weaknesses in existing security measures (e.g., the use of outdated software and protection measures with vulnerabilities that have not been patched)?
- iv) Were there weaknesses in the use of portable storage devices or connectivity to the Internet?
- v) Were the methods for accessing and transmitting personal data sufficiently secure (e.g., access limited to authorized personnel only)?
- vi) Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data?
- vii) Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data?
- viii) Was there a clear line of responsibility and communication during the management of the data breach incident?
- ix) Were pre-defined modes of communication effective during the data breach incident response?

b) Resource Related

- i) Were there enough resources to manage the data breach incident? Should external resources be engaged to better manage such incidents?
- ii) Were key personnel given sufficient resources to manage the incident?

c) Employee Related

- i) Were employees sufficient aware of security related issues?
- ii) Was training provided on personal data protection matters and incident management skills sufficient?
- iii) Were employees informed of the data breach incident and the learning points from the incident?

d) Management Related

- i) How was senior management involved in the management of the data breach incident?

- ii) Was there sufficient or effective direction given in managing the data breach incident?

5. Resources

This Standard should be read in conjunction with the following documents:

- Group Risk Governance Framework
- Data Management Policy
- Group Privacy Policy
- Group Privacy Standard

6. Review

This Standard will be reviewed once annually or when there is a major change, with changes approved by the Group CRO. Where no changes to the Standard are proposed after the annual review, Group CRO must still be informed that a review has been conducted.

Appendix - Notification of Data Breaches to The Monetary Authority of Singapore (“The Authority”)

The MAS has issued the following regulatory requirement on notification of data breach incidents to the MAS.

MAS Circular No. ID 10/14

“2 The Authority” sets out below the revised expectations for licensed insurers regarding the expectations for notifying “the Authority” of data breaches, as defined under the PDPA 2012.

- (a) “The Authority” should be concurrently notified of data breaches that are required to be notified to PDPC.
- (b) “The Authority” should be notified of data breaches that meet the criteria under MAS Notice 127 and the Authority’s Guidelines on Outsourcing, based on the timelines indicated within these instruments.
- (c) For data breaches that fall outside paragraphs 2(a) and 2(b), the Authority should be notified of them on a consolidated basis, within 3 weeks from the last day of each quarter. The breaches to be included should be those identified during the quarter. The notification should contain, for each data breach, on a best effort basis:
 - i. a description of the incident and how it was discovered.
 - ii. an analysis of the root cause of the incident and the key control deficiencies.
 - iii. an assessment of the impact of the incident (e.g., number of customers affected, financial and non-financial impact).
 - iv. a description of the remedial measures taken to manage the incident, including the extent of service recovery performed or the insurer’s reasons for deciding not to perform service recovery; and
 - v. a description of the controls to be implemented to prevent occurrence of similar incidents. Where there are updates to any of the details in paragraph 2(c) after the initial notification of the data breach, these should be provided together with the subsequent quarter’s notification to the Authority.