Horizon Specialist Contracting Ltd
www.horizonsc.co.uk

Data Protection Breach Policy/Reporting Procedure

Reviewed September 2020

Security Classification:

Not Protected

Approval History

Version No	Approved by	Approval/Review Date	Comments
V1.0	Louise Kerry-Armes	2.2.2018	Initial Review
V1.0	LKA	12.12.2018	Annual review
V1.0	LKA	10.92019	Annual review
V1.0	LKA	29.9.2020	Annual review

Document Author/Owner

Version	Authors	Role
V1.0	Central IT	Implement/Review

Document Governance

Next Review Date	September 2021
Published to	Intranet only
Circulation	This framework is to be made available to all Horizon SC staff and observed by all members of staff
Information Classification	NOT PROTECTED

Index

1. INTRODUCTION

1.1 Background

1.1.1 Due to the introduction of the General Data Protection Regulation (GDPR), which is being adopted by Horizon Specialist Contracting Ltd (Horizon SC), the GDPR requires that Horizon SC provides assurance that appropriate procedures are in place for the handling of security incidents involving Personal Data. The GDPR's purpose is to enable organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

1.2 Purpose

1.2.1 The purpose of an incident response is to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently
- Incidents are assessed and responded to appropriately. Ensure action is taken to reduce the impact of disclosure
- Mitigation improvements are made and are put in place to prevent recurrence. Serious breaches can be reported to the Information Commissioner's Office
- Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents

1.3 Intended Audience

1.3.1 The intended audience for this document is anyone involved in responding to security incidents.

1.3.2 It is assumed that the readership has a good understanding of the key aspects of privacy legislation and best practice when managing such incidents.

1.4 Scope

1.4.1 This procedure applies to all staff, partners, shared services, suppliers, contractors, representatives and agents of Horizon SC who process personal data for which Horizon SC is either the data controller or has an interest in the personal data affected.

1.4.2 All staff have a role to play to ensure a safe and secure workplace.

1.5 Terminology

1.5.1 In line with International Organisation for Standardisation (ISO) directive on the use of terminology in standards and for the avoidance of doubt the following words have the specific meanings as described below when used in this document:

- ‘Shall’ or ‘Must’ denote a mandatory requirement. Deviation from these shall constitute non conformance
- ‘Shall Not’ or ‘Must Not’ denotes something that is prohibited
- ‘Should’ denotes a recommendation that is non mandatory
- ‘Should Not’ denotes something that is not recommended
- ‘May’ denotes something that is optional

2. INCIDENT MANAGEMENT

2.1 Definition

2.1.1 A Data Protection breach is the result of an event or series of events where Personally Identifiable Information (PII) is exposed to unauthorised or inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the PII.

2.1.2 Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

2.1.3 Examples of common incidents are listed below:

Type	Example
Technical	Data Corruption Malware Corrupt Code Hacking
Physical	Unescorted visitors in secure areas Break-ins to sites Thefts from secure sites Theft from unsecured vehicles/premises Loss in transit/post
Human resources	Data Input errors Non-secure disposal of hardware or paperwork Unauthorised disclosers
Inappropriate Sharing	Copying & sharing data without consent

2.1.4 The pro forma at Annex A is to be used for the reporting of ALL suspected data protection breaches

2.2 Management Statement of Intent

2.2.1 Horizon SC shall:

- Put measures in place to ensure that awareness of data protection will enable breaches to be reported more easily
- Issue guidance on how to report PII breaches for analysis, categorisation and response
- Provide resource to analyse reported PII breaches to identify those that are incidents requiring a structured response
- Assemble a breach response team with defined responsibility, as required, to contain and recover from security incidents
- Ensure that its contemporaneous logs of incidents are kept

- Hold periodic post resolution lessons learned meetings to focus on trends and improvements to reduce the likelihood and impact of recurrence, as appropriate.

2.2.2 Horizon SC recognises that in some instances PII breaches are beyond its reasonable control and the importance of being prepared for such eventualities.

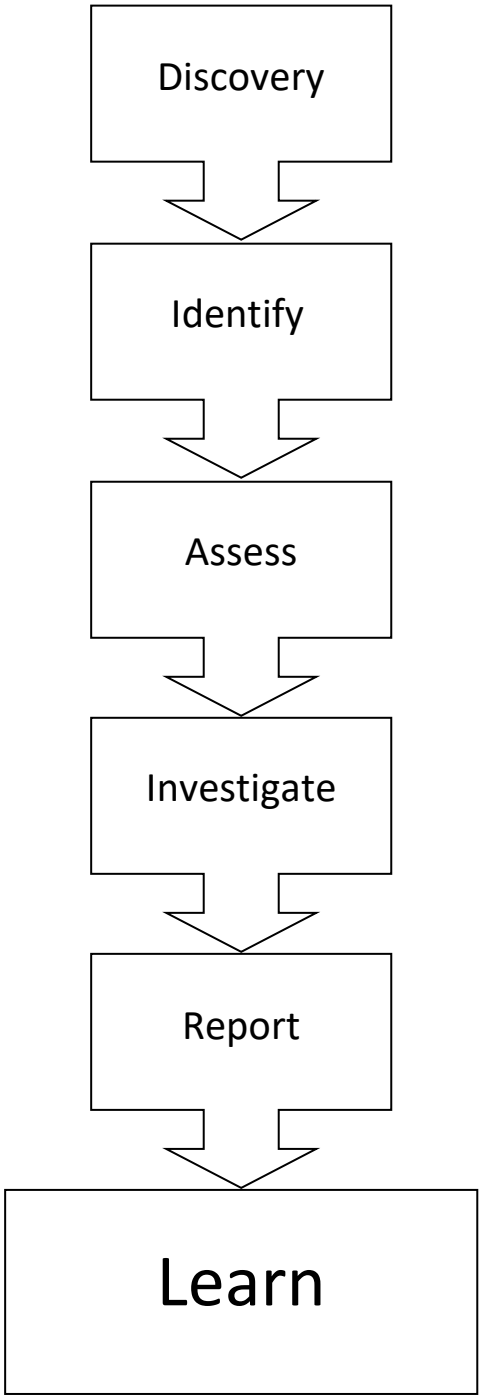
2.2.3 Horizon SC shall ensure that it reacts appropriately to any actual or suspected PII breaches occurring either within the Company and its systems or with data processors.

2.2.4 Horizon SC recognises that a structured response to PII breaches has a number of clear benefits to it including:

- Improving overall PII security
- Reducing adverse business impacts
- Strengthening the PII breach prevention focus and strengthening prioritisation
- Strengthening evidence collection and custody arrangements
- Contributing to budget and resource justifications
- Improving updates to information governance risk assessment and risk management
- Providing PII security awareness and training material
- Providing input to PII security policy reviews via lessons learned

2.3 Outline Process for incidents

2.3.1 Diagram below shows the flow of actions involved in a PII Breach Investigation



2.3.2 Discovery/Identify/Assess/Investigate - Breaches and weaknesses need to be reported at the earliest possible stage to the Data Protection Officer (DPO) (within 72hrs) in the form of Annex A. Only in urgent circumstances, can incidents be reported in other ways.

2.3.3 Following notification, the DPO (Data Protection Officer) will open an incident log and make an initial assessment of the breach's severity. Once that's known, the DPO must make the highest level of management aware. HR will be informed if deemed applicable.

2.3.4 The reporting form should capture most of the information needed to establish the scope of a breach but there will be a need to obtain additional information about the event, the assets affected, determining the type of incident, its category and priority before putting together an incident response team to manage the incident.

2.3.5 This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible to determine how the breach occurred, what actions have been taken, whether outside agencies are involved and whether the data subjects have been notified.

2.3.6 Not all data protection breaches will result in formal action. Some will be false alarms or "near miss" events that do not cause immediate harm to individuals or the organisation. These should still be reported, as analysis of these will allow lessons to be learnt and continual improvement.

2.4 Reporting

2.4.1 The objective of any breach investigation is to identify what actions the organisation needs to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be reported to the Information Commissioner's Office. The purpose of the report is to document the circumstances of the breach, what actions have been taken, what recommendations have been made and whether the disciplinary action process needs to be followed.

2.5 Lessons Learned

2.5.1 Key to preventing further incidents is ensuring the organisation learns from an incident. Regular review meetings will take place chaired by the DPO to agree recommendations and each Breach Report will be shared with the relevant Director/s.

2.6 Review and Revision

2.6.1 This document will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

2.7 Key Message

2.7.1 A culture in which data protection breaches are reported should be fostered. Although sanctions cannot be totally ruled out, the key objective is to develop valuable insight into how such events occur and staff need to be assured that reporting a breach will not in itself result in disciplinary action.

3. OUTLINE PROCEDURE FOR INCIDENT HANDLING

3.1 Investigation

3.1.1 Once a breach has been reported in the form of Annex A the following actions must be carried out by the DPO as soon as possible:

- Create an entry in the Company's Personal Data Incident Log using the information provided by the reporter
- Create a folder under Data Breaches using the following format – PB[Breach Reference Number]
- Start an investigation report and save it in this folder together with any emails/documents relating to the breach.

3.1.2 Inform the relevant Directors and prepare a report for the Breach Review Meeting if required.

3.1.3 If the Breach Review Meeting concludes that a report to the ICO is required, contact the relevant Director/s to seek approval for notification. An initial report for the ICO should also be prepared.

3.1.4 Consideration must be given to notifying the individual(s) affected by the breach. Factors to consider include:

- Sensitivity of information
- Volume of information
- Likelihood of unauthorised use
- Impact on individual(s)
- Feasibility of contacting individuals

3.1.5 Any notification must be agreed by senior managers of reporting business unit and if required, legal services and communications.

3.1.6 Begin investigation and complete report as soon as possible

4 INCIDENT REVIEW

4.1 A key part of data protection breach management is a process of continual review. Every two to four weeks the DPO and relevant Director/s meet to review current breaches. The purpose of these meetings is to provide an update on the progress of any investigation, discuss possible recommendations and consider whether specific incidents should be reported to the ICO.

4.2 These meetings are used to review the outcome of any investigations, as appropriate, and examine the recommendations made and discuss information governance matters. Following on from these meetings, a monthly brief is given to management members giving an overview of current information issues and breaches which are then escalated to the Managing Director if required.

5 RECOMMENDATIONS

5.1 Regardless of the type and severity of incident, there will always be recommendations to be made even if it is only to reinforce existing procedures. There are two categories of recommendation that can be made:

> **Local** – these apply purely to the department(s) affected by the incident and will usually reflect measures that need to be taken to restrict the chances of the same type of incident occurring.
> **Corporate** – some incidents will be caused by factors that are not unique to one department but can be found right across the organisation. Issues such as training, information handling and physical security affect all departments and it is essential that the organisation identifies such risks and puts in place measures to prevent the incident occurring elsewhere. Corporate recommendations may even be shared regionally especially where it relates to policies/protocols in use by a number of public bodies.

5.2 All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the organisation puts in place whatever measures have been identified and that there is an individual that can report back to management members regarding progress. The second is that where incidents are reported to the ICO, the Company can demonstrate that the measures have either been put in place or that there is a documented plan to do so.

5.3 This is a recurrent theme of ICO enforcement and it's important that the organisation's procedures reflect this. Identifying recommendations is more than just damage control – the knowledge of what has happened together with the impact is a fundamental part of learning which can then be disseminated throughout the organisation and beyond.

Annex A – Data Protection Breach Reporting Form

The aim of this document is to ensure that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to customers and/or Horizon SC data and information and the individuals concerned.

The checklist can be completed by anyone with knowledge of the incident. It will also require review by the DPO who can determine General Data Protection Regulation implications and assess whether changes are required to existing business processes.

1. Summary of Incident	
Date and Time of Incident:	
Number of people whose data is affected:	
Department:	
Nature of breach e.g. theft, disclosed in error, technical problems:	
Description of how breach occurred:	

2. Reporting	
When was the breach reported?	
How did you become aware of the breach?	
Has the Data Protection Officer been informed?	

3. Personal Data	
Full description of personal data involved (without identifiers):	

Number of individuals affected:	
Have all affected individuals been informed? If not, state why not:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	

4. Data Retrieval	
What immediate remedial action was taken?	
Has the data been retrieved or deleted? If yes please state the date and time:	

5. Impact	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details:	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed?	

If so, please provide details:	

6. Management	
Do you consider the employee(s) involved has breached information governance's policies and procedures?	
Please inform of any disciplinary action taken in relation to the employee(s) involved:	
Had the employee(s) completed data protection training?	
As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities?	
Has there been any media coverage of the incident? If so, please provide details:	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure:	