HORIZON
STRATEGIC PARTNERS

Business Continuity Plan – Data Security

Horizon Strategic Partners Ltd act as a Data Processor for a number of organisations where varying levels of personal and/or confidential data is processed.

1. Purpose and Scope
    a. This document contains the procedures and plan that should be used when dealing with a data-security breach where HSP is a Data Processor for the data affected.
    b. We should endeavour to ensure that any affected systems are operational again within 48 hours.
    c. Acceptable recovery conditions will be documented in the applicable system contract, but will typically include minimal data loss and full disclosure to the customers.
    d. This plan is required if a sub-processor of HSP processed data reports to us that they have suffered a data-breach that may have affected our system(s).
2. Responsibilities
    a. Director Eamus Halpin is the key staff member to be involved. He is the main decision-making authority and also has authority to spend additional funds in the case of emergency requirements.
3. Plan Invocation
    a. This plan should be invoked for any data-breach relating to Horizon Strategic Partners Ltd's systems where Personal and/or Confidential data is processed.
    b. The first HSP employee to become aware of the data-breach (either because they discover it themselves, or they receive a notification from a supplier) should raise it with EH asap.
    c. The response team will vary depending on the system(s) involved, but EH should setup a dated "data-breach" channel on Slack and ensure everyone necessary is added to the channel and acknowledges their presence. This slack channel (both text and voice conferences are available) will last as long as the team is mobilised.
    d. The team should stand down once all outstanding actions as a result of the breach have been resolved and final responses have been received from any participating third parties (eg suppliers and/or customers)
4. The Plan
    a. Start a timer as soon as we are reasonably sure a breach has taken place. We have 72 hours to report it to the Data Controllers.
    b. Based on which system(s) are affected and the staff available, identify an individual to act as co-ordinator for each affected system.
    c. Classify the severity of the breach based on the personal / confidential data that has been compromised. If any special-category (eg health) data has been breached then it must be classed as HIGH risk. Use the Processing Activities document to help.
    d. Review the contract for the affected system(s) to establish what the recovery objectives are and what is necessary to achieve them.
    e. Work with the sub-processor to prevent any further access to the system until it is established that the breaching party no longer has access to the data. If this cannot be established, consider building a separate "clean" environment. Discuss with sub-processor and decide what to do based on severity of breach and processor / sub-processor confidence.

f. Ensure all knowledge gained and all decisions made are logged in the Slack breach channel.
g. Draft a communication containing full details of the breach (timescales, number of records, risk / type of data breached)
h. Notify all data-controllers affected of the breach within 72 hours of the initial discovery.
i. Work with the data-controllers involved to ensure their questions are answered and their own breach policies are supported accordingly.
j. Identify any actions that HSP Ltd could deliver to reduce the chances of this kind of breach happening I future.
k. Ensure the resulting actions are dealt with in a suitable timeframe following the breach.

5. Document Details (Owner, Approver, Change History)

The document has been written by Software Development Manager, Dave Russell.

Version	Description	Approval	Issue Date
1	Initial Version	EH	25/3/2019

HORIZON
STRATEGIC PARTNERS

Example Scenario

What role do processors have?

If your organisation uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform you without undue delay as soon as it becomes aware.

Example

Your organisation (the controller) contracts an IT services firm (the processor) to archive and store customer records. The IT firm detects an attack on its network that results in personal data about its clients being unlawfully accessed. As this is a personal data breach, the IT firm promptly notifies you that the breach has taken place. You in turn notify the ICO.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the GDPR.

If you use a processor, the requirements on breach reporting should be detailed in the contract between you and your processor, as required under Article 28. For more details about contracts, please see our draft GDPR guidance on contracts and liabilities between controllers and processors.