**Data breach**

**Policy, process and procedures**

Evolve Intervention Data Breach Assessor:

**Emma Prince –** [**e.prince@evolve-intervention.com**](mailto:e.prince@evolve-intervention.com) 01245 526069

**Contents**

**Introduction**

**Personal data definition**

**Data breach definition and examples**

**Procedure**

**Process flowchart**

**Notification**

**Record keeping**

**Introduction**

Evolve Intervention is committed to the safe handling, storage and sharing of all the data it is responsible for. Whilst there are processes in place to minimise the possibility of a data breach occurring we have to be prepared for one so that in the unlikely event of one occurring we are ready to respond. If a data breach does occur, it is important to move quickly to identify the extent and severity of the breach and the risk that it poses to the data subject(s) to which the breached data relates.

**Personal data definition**

A data breach is concerned with personal data so it is necessary to define what this is. Personal data is described by the General Data Protection Regulations (GDPR) as: Any information relating to an identifiable person who can be directly or indirectly identified, in particular in reference to an identifier (see [Information Commissioner’s Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/) (ICO) for more detail), this can include records that have been pseudonymised e.g. where reference numbers instead of names are used.

**Data breach definition**

A data breach is defined as when personal data is either:

* Lost
* Destroyed
* Corrupted
* Disclosed
* Accessed or passed on by an unauthorised person
* Made unavailable e.g. if encrypted through ransomware

As soon as you are aware that a security incident has happened you need to establish whether a personal data breach has occurred and if so you need to follow the procedure for reporting

**Examples of data breaches**

Below are examples of potential breaches, please remember these are not exhaustive – there will be many other instances that constitute a breach - but these aim to provide some real-world examples to aid your understanding:

* You accidently email a young person’s records to the wrong person
* You lose some papers from your bag on the way to a meeting
* Someone hacks into the supplier of our case management system or cloud storage area
* You leave your laptop displaying a client record in a room with a non-authorised person present
* A client record is accidently deleted
* There is an error with the HR system and records become available to those not authorised to view them
* Staff supervision notes are stored in a way that allows other workers to view them
* Supervision notes are stored in a password protected format but the password has been forgotten

In these and any other potential breach situations care should be taken to follow the process of dealing with the breach, including reporting the breach to the ICO if necessary.

**Procedure for dealing with a security incident / personal data breach**

When you are aware that a security incident has taken place, whether or not you consider this to be a personal data breach you should report this to the Evolve Intervention Data Breach Assessor (EIDBA) so that details can be taken, a record made and a decision taken as to whether this is a personal data breach and if so of what severity. It is important that you notify the EIDBA within 6 hours of the potential breach being discovered as there are time limits imposed by law for the reporting of such incidents.

Once the EIDBA has been notified they need to decide if the incident is a personal data breach. If the incident is not considered to be a personal data breach then:

* Obtain all the relevant information needed to record the incident in the data breach database
* Record the incident:
  + Details (what, when, how etc)
  + Effect of the incident
  + Assessment details and decision (why is it not a personal data breach?)
  + Learning points / actions – how can this be prevented in the future?

If the incident is considered a data breach then a decision needs to be taken as to whether the incident needs to be reported to the ICO, using the following questions as a guide to this assessment:

* Is the breach likely to put at risk people’s rights and freedoms?
* What is the severity of the risk to people’s rights and freedoms?
* What are the potential negative consequences / risks to personal rights and freedoms for the data subject? E.g.
  + Loss of confidentiality
  + Potential of harm occurring (physical, emotional or material)
  + Risk of identity theft / fraud
  + Loss of control over personal data

If the breach is **likely** to put rights and freedoms at risk then the ICO must be notified within 72 hours of someone becoming aware of the incident having occurred. Guidance on how to report to the ICO can be found further on in this document.

There also needs to be an assessment to determine whether the data subject(s) that the breach relates to should also be informed of the breach. The test for assessing whether to inform individuals is similar to the one for assessing whether to inform the ICO, except the test is whether there is a **high** risk, rather than just a risk to rights and freedoms. If it is decided that the data subject(s) do need to be informed then this needs to be done without delay in order that they can take their own mitigating actions to avoid any impact to their rights and freedoms.

The breach also needs to be recorded on the data breach database - whether or not the ICO is to be informed – it is the responsibility of the EIDBA to ensure accurate records are kept on the database. The records should include the following information:

* Details
* Effect
* Actions taken to mitigate negative consequences to data subjects
* Actions taken to mitigate future occurrences
* Assessment details and decision (why is this being reported / not reported to the ICO?)
* Date reported to ICO
* Decision to inform data subjects (Yes / No and why)
* Date individuals informed

**Process for dealing with a security incident / data breach**

Is the security incident a personal data breach?

No

Yes

Does it need to be notified to the ICO (follow assessment procedure)?

Determine the cause(s) of the incident and any mitigating actions to prevent a repeat. Record the incident, assessment and any learning / follow up actions in the data breach database

Yes

No

Security incident

Record the breach on the data breach database, including all the criteria cited in the data breach procedure and the decision **to not inform the ICO**.

Gather all information needed and inform ICO of breach within 72 hours

Do(es) the data subject(s) need to be informed of the breach?

Implement any mitigating actions to minimise risk of future occurrences e.g. staff training, supplier change, policy and procedure review.

Yes

No

Record the breach and decision to **inform ICO but not data subject(s)** on the data breach database, including all the criteria cited in the data breach procedure.

Inform data subject(s) of breach

Record the breach and **decision to inform ICO and data subject(s)** on the data breach database, including all the criteria cited in the data breach procedure.

**Notification of a breach**

When a data breach has been assessed as needing to be notified to the ICO the guidelines on the ICO website should be followed: [Report a breach](https://ico.org.uk/for-organisations/report-a-breach/) or call them on 0303 123 1113. Notification needs to be made within 72 hours of the discovery of a breach, even if not all of the information is available it is better to report it sooner and then update the ICO once you have more information.

**Recording a security incident, possible data breach or a data breach**

An excel spreadsheet should be used to record any security incidents, possible data breaches or data breaches. The recording of any data breach incidents whether possible or actual is mandatory under the GDPR and must be completed – it is the responsibility of the EIDBA to ensure that the records are added and that an accurate reflection of any incidents or assessments is recorded in a timely manner.