COM015 – DATA BREACH POLICY & PROCESS v01.00

Table of Contents

1 Introduction

1.1 This document applies to all staff and Members of the Scottish Legal Complaints Commission ('the SLCC'), including the SLCC's Consumer Panel, which is an independent advisory Committee, established by the Legal Profession and Legal Aid (Scotland) Act 2007.

1.2 This document also applies to Mediators, External Reporters and those data processors who process personal data on behalf of the SLCC.

1.3 This document explains the SLCC's policy and process to be followed in a situation where the following action(s) / failure(s) in respect of personal data held by the SLCC might have occurred:

- Loss
- Unauthorised disclosure
- Unauthorised access
- Deliberate action / inaction
- Accidental action/ inaction
- Release of data to an incorrect person / body
- Devices stolen / lost
- Theft of personal data
- Alteration of data without permission
- Loss of availability of data

1.4 The SLCC's IT Security Policy (OM013) refers in more detail to the action which should be taken in a situation where there has been a specific IT security breach and the processes which the SLCC has in place to deal with such matters.

1.5 The SLCC's Business Continuity Plan (GOV015) also provides information about the action and personnel who are likely to be involved in the event of an IT or premises failure.

1.6 The SLCC's Privacy Policies can be found at www.scottishlegalcomplaints.org.uk/privacy.

1.7 The application of this policy and process aims to ensure:

- Conformation to the SLCC's policy and processes.
- Early reports of incidents, sufficient to decide appropriate escalation routes, notification and communication to the relevant parties.
- Consistency in the approach to evaluating breach incidents.
- Appropriate action is taken to prevent damage, distress and concern to data subjects and to maintain the reputation of the SLCC.
- Appropriate corrective action can be taken to prevent recurrence of the incident.
- Lessons learned can be identified and communicated.
- Transparent reporting of incidents to the Supervisory Authority.
- Appropriate records are kept of breach incidents

2 Information Security Statement

2.1 The SLCC recognises the value and importance of its information resources, and its statutory obligations to protect them against, for example, unauthorised destruction, corruption or loss. The SLCC will actively protect these assets in ways that are appropriate, proportionate and cost effective. In doing so the SLCC will fulfil its statutory responsibilities to protect the data it holds about and on behalf of all stakeholders, and maintain the effectiveness and continuity of its services.

2.2 Every individual working for the SLCC who have access to its information systems has a responsibility to protect that information and prevent harm to all stakeholders. Information security is primarily about and for people, not technology.

2.3 The SLCC is committed to ensuring that its data processing activities are carried out in accordance with the General Data Protection Regulation ('the GDPR'), and that it has in place policies and procedures that will enable an individual to exercise the rights that are available to them under data protection law and regulation.

2.4 **The SLCC will:**

- Operate security governance to ensure senior management direction and promote compliance with the GDPR throughout the organisation.
- Ensure that controls are based on business requirements and are balanced against risk assessments that are reviewed on a regular basis.
- Maintain an effective, properly resourced information assurance group to monitor controls and assist user departments to safeguard their data.
- Carry out Data Privacy Impact Assessments (DPIAs) where appropriate, with a view to minimising privacy risk in relation to data processing activities. DPIAs will reassure individuals that the SLCC has followed the best practice and reduce the risk of data security breaches from occurring.

2.5 **To support this, the SLCC must:**

- Make sure that appropriate data is collected and then properly maintained and processed, and that its confidentiality and integrity are suitably preserved.
- Protect our information systems from a wide range of physical threats to minimise risk and maximise their value to the SLCC.
- Detect and protect against viruses and other malicious software, and correct security vulnerabilities.
- Protect critical business processes and online services against failures and disasters.
- Educate and train our data processors to handle and process information securely, effectively and legally.
- Develop controls by a process of continuous monitoring and measure their effectiveness.
- Report all breaches of information security, actual or suspected, and deal with them in an appropriate manner.
- Conduct regular DPIAs, audits and training plans.

3 Consequences of a data breach

3.1 A data security breach leading could damage the SLCC's reputation and its relationship with its stakeholders. It could cause harm and distress to individuals who are affected by the breach, exposing them to serious risks to their personal safety, fraud, identity theft and embarrassment, especially in circumstances where the personal data in question is of a sensitive nature (referred to as 'Special Category' data), such as data relating to any of the following:

- Race
- Ethnic origin
- Politics
- Religion
- Trade Union Membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life
- Sexual orientation

3.2 The SLCC could also be sued by a data subject affected by the data breach and / or fined by the Information Commissioner ('the ICO'), potentially up to €20 million (and an additional €10 million for failing to report a data breach to the ICO, in circumstances required by the GDPR.

4 Appointment of a Data Protection Officer

4.1 As a Non Departmental Public Body, the SLCC is required to appoint a Data Protection Officer ('DPO') under the GDPR.

4.2 The DPO has certain defined obligations, one of which being to report to the highest management level of the organisation.

4.3 The DPO must have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. It is the duty of the DPO to inform and advise the Data Controller of their obligations under the GDPR, to monitor compliance, provide advice and to act as a contact point for the Supervisory Authority ('the ICO').

4.4 The benefits of a DPO are:

- Creates more **TRANSPARENCY** with stakeholders, employees and the Regulator
- Creates new level of **ACCOUNTABILITY** within the SLCC for the privacy framework
- **CONTROL** in the environment which underpins how information is managed
- **SINGLE POINT OF CONTACT** to embed privacy and data by design
- Ensure **COMPLIANCE** with the law/regulation in a **PRACTICAL** way, in tandem with operational efficiency and effectiveness

- **INSURANCE** – the DPO acts as check and balance on interests of data subject –v- the interests of SLCC. The DPO can police internal proposals and manage issues or events which, if handled poorly, can leave the SLCC open to censure / fine by the ICO

- **TRAINING & DEVELOPMENT** from a single, well intentioned and informed coach.

5 Accountability for data breaches

5.1 The SLCC's Chief Executive Officer ('the CEO') as Data Controller has overall responsibility for management of any breach of personal data.

5.2 In the absence of the CEO, the responsibility for management of the breach shall fall to the next most senior member of staff.

5.3 Operational management of the breach will usually be delegated to the appropriate person/s from the Data Breach Response Team.

6 Data Breach Response Team

6.1 The SLCC has identified the following roles as being required for inclusion in the Data Breach Response Team ('the DBRT'):

- Chief Executive Officer (CEO)
- Data Protection Officer (DPO)
- Information Officer (IO)
- Facilities Officer (FO)
- HR Manager (HRM)
- Communications Officer (CO)

6.2 The specific nature of the data breach incident will dictate who from the DBRT will need to be involved in any action and at what particular stage of the data breach process.

6.3 The DPO should be informed of all data breaches for logging purposes, even if the action to be taken does not require the DPO's involvement, e.g. if the breach relates to an HR or facilities issue, which would be better managed by the HRM or FO, or in circumstances where the DPO is unavailable to deal with a data breach incident and action requires to be taken in their absence.

6.4 The DPO will report to the DBRT every 6 months (to co-incide with the DPO's Board update). This will ensure that the DBRT is kept updated on a regular basis about all data breach activity. Sharing outcomes through reporting should identify learning points and training needs for the SLCC's data processors. It will also highlight any training needs for the DBRT insofar as this relates to the application of the Data Breach Response Plan.

6.5 If there is a sudden escalation in data breaches, or if a serious breach occurs which may put the SLCC at serious reputational or financial risk, the CEO should be informed immediately.

7 Data Breach Response Plan

7.1 There are **four** important elements to the Data Breach Response Plan:

1. **Preparation** – the SLCC has carried out an information audit (which records what personal data the SLCC holds, why we have it, where it is stored and who has access to it). Breach reporting processes have been put in place and the DBRT has been established and appropriately trained. The SLCC's data processors have been informed of the requirements of the GDPR and the importance of data security and breach reporting.

2. **Detection, analysis and assessment of risk** - any risks associated with a breach incident should be assessed, as these are likely to affect what steps are necessary once the breach has been contained. In particular, there should be an assessment of the potential adverse consequences for individuals, how serious or substantial these are, and how likely they are to happen.

3. **(a) Containment, eradication and recovery** - the response to the incident should include a system back-up and recovery plan and, where necessary, procedures implemented for damage limitation.

3. **(b) Investigating and reporting** - information should be assimilated and investigated by the appropriate person(s). Evidence should be interrogated and protected and where appropriate, people should be notified about a data breach. It is necessary to be clear about who needs to be notified, why and when notification should take place.

4. **Post-incident activity, evaluation and response** – it is important that there is a thorough investigation of the causes of the breach and an evaluation of the effectiveness of the response to it. Lessons learned are to be fed back to the appropriate person(s) / line manager(s). If necessary, there should be an update to policies and procedures to minimise / avoid recurrence of the breach in the future. Training needs should be identified and rolled out across the organisation.

7.2 The DPO is required to keep a Data Breach Log, which will record the following:

- Date DPO notified
- Breach type
- Details of the incident
- Special Category Data
- Person(s) involved
- Report required to data subjects
- Report required to ICO
- Justification for not reporting to ICO
- Dates of contact with data subjects / ICO
- Outcome / remedial action taken
- Follow-up action

8 What to do if a breach occurs?

8.1 On becoming aware of a breach or a potential breach of data security it is vital to ensure that it is dealt with immediately and appropriately, to minimise the impact of the breach.

8.2 The GDPR has introduced an obligation to **notify** certain data breaches to the ICO **without undue delay** and, where feasible, **within 72 hours** after the data controller has become aware of the data security breach. If notification is later than 72 hours, justification must be provided for the delay. It is vital, therefore, that as much information as possible is obtained in the first few days of the breach being identified.

8.3 **What constitutes a data breach incident?**

Any of the actions referred to in the **Introduction** could potentially amount to a personal data breach.

8.4 Suspected incidents, i.e. "near misses" should also be notified to the DPO, as lessons can be learned from this information.

8.5 **What incidents need acting upon?**

Any incident where personal data might be affected. It will be for the DBRT to decide whether the breach is likely to result in *"a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautionary measures"*. In those cases, it is likely that the breach will need to be reported to the ICO within 72 hours.

8.6 **What incidents can be ignored?**

None - unless personal data is not involved. At the very least, a report of a suspected incident should be reported to the DPO, so the incident can be logged and triaged as appropriate. Only the DBRT should make the decision as to whether an incident should be ignored (until such a time as a bank of incidents has been assimilated and assessed and risks negated for a particular type of incident).

8.7 **Action to be taken by SLCC staff / data processors**

YOU MUST TAKE ACTION AS SOON AS YOU ARE AWARE OF A PERSONAL DATA BREACH. FAILURE TO DO SO COULD LEAD TO DISCIPLINARY ACTION

[There is a flow chart at Appendix 1, which provides a simple illustration of the action which should be taken in the event of a personal data breach].

8.8 As soon as a data breach incident (or suspected incident) has been identified, notification must be provided to the DPO / IO (or any other member of the DBRT if the DPO / IO are unavailable) without delay. For SLCC staff, their line manager should also be informed. **It is the responsibility of the person who receives information about a data breach or suspected**

data breach to take the appropriate action.

8.9 If the DPO / IO are unavailable, i.e. you receive an out of office message, notification should be sent to the SLCC's Enquiries inbox, so that this can be passed on to the next most appropriate person from DBRT. If it is not clear who is the appropriate person, notification should be sent to the CEO, as Data Controller.

8.10 The DPO / IO (or other appropriate person in their absence) will send an email reply as soon as possible, acknowledging notification of the breach. Attached to the email will be a Data breach evaluation form (*at Appendix 2*), which must be completed on receipt, and emailed back to the person from whom it was received (for SLCC staff, this should also be cc'd to their line manager.

8.11 The appropriate person/s from the DBRT will evaluate the form and assess what next steps are required. Further information / evidence relating to the data breach may be required to be provided. No evidence should be destroyed at this stage.

8.12 The person reporting the breach may be required to attend a meeting with the DPO / IO to supply more information about the breach incident, if requested. They may also be asked to contact data subjects themselves, for more information or to advise that a breach has occurred. Advice and Assistance will be provided by the DBRT. It is, however, incumbent upon the person responsible for the breach to take responsibility for action.

8.13 **Action to be taken by DPO / DBRT**

The first step will be to establish who, from the DBRT, are likely to be required to be involved in a particular data breach incident. It is most likely that this will be the DPO / IO. However, it might be necessary for other members of the DBRT to be involved, particularly in circumstances where the DPO / IO are unavailable.

8.14 Following receipt of the Data breach evaluation form, the DPO / IO will proceed to complete the Data breach assessment form (*at Appendix 3*) as soon as possible.

8.15 The guide to assessing the severity of the breach forms provides assistance in reaching the decision about the next steps which might require to be taken.

8.16 As part of the assessment of the breach incident, consideration must be given to whether the breach is likely to result in a risk to the rights and freedoms of the individual(s) who are affected. This will include consideration of whether, if unaddressed, the breach is likely to have a significant detrimental effect on the individual(s) affected such as could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.

8.17 When it is considered that the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the personal data breach shall be communicated to the data subject(s) affected by the breach **without undue delay**. The DPO / IO will decide whether that communication should be made by themselves, by the notifying person or by another appropriate

person, e.g. a line manager / CEO.

8.18 When it is considered that the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the personal data breach shall be communicated to the data subject(s) affected by the breach **without undue delay**. The DPO / IO will decide whether that communication should be made by themselves, by the notifying person or by another appropriate person, e.g. a line manager / CEO.

8.19 The individual(s) concerned shall be provided with the following information:

- a description of the nature of the breach, in clear and plain language
- the name and contact details of the DPO (or other contact point where more information can be obtained);
- the consequences of the personal data breach;
- the measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate possible any adverse effects.

8.20 Where, following consideration of the nature and circumstances of the breach, it is considered that the breach may result in a risk to the rights and freedoms of the individual(s) who are affected, the breach will be reported to the ICO without undue delay and no later than 72 hours after having first become aware of the breach.

8.21 In circumstances where there has been media interest in a breach incident, or in circumstances where the SLCC considers it necessary / appropriate to make a press statement on a particular incident, the CO should prepare the appropriate proactive or reactive press statement for approval by the CEO. Thereafter, there should be active monitoring of media and social media and appropriate feedback provided to the CEO / DPO.

8.22 **Evaluation, preventative action and follow up**

Where a data breach has occurred, the DPO (or appropriate member of the DBRT) will complete the Data breach follow up form (*at Appendix 4*).

8.23 In most cases, the CEO and DPO will invite the appropriate individual(s) to a meeting to discuss the breach incident. Thereafter, the CEO and DPO will decide what follow up action should be taken, with a view to minimising or avoiding the risk of the breach occurring in the future.

8.24 Where the breach involves an individual from the SLCC's staff, that person's line manager will also be invited to attend the meeting. It might also be necessary for another member of the DBRT to attend the follow-up meeting, depending on the nature of the data breach.

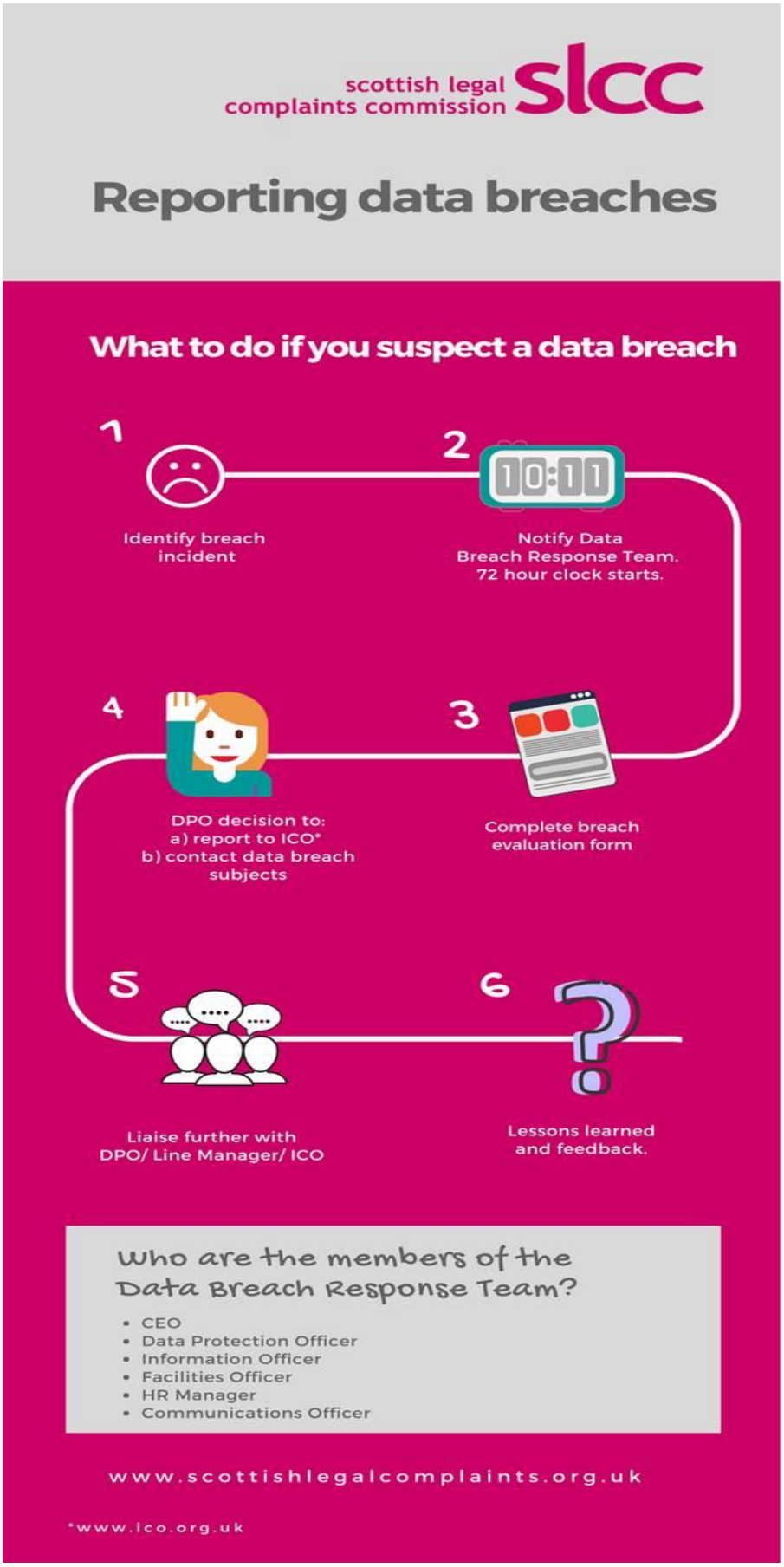
8.25 Lessons learned and training should be rolled out to all staff and / or data processors, as appropriate. Consideration will also be given to the need for existing policies and procedures to be amended, in light of the particular circumstances of the data breach incident.

8.26 In assessing what steps require to be taken to prevent further breaches from occurring, consideration shall be given to any decision and / or recommendations of the ICO, in circumstances where the ICO has been notified of the breach.

8.27 The DPO will review (and report to the Board) the following KPIs on a 6-monthly basis:

1. Time taken to detect the incident
2. Time taken to report the incident to the DBRT
3. Number of false positives
4. Security tools used to spot the incident
5. Number of negative recommendations from ICO

Appendix 1 – Data Breach Infographic



scottish legal complaints commission slcc

Data breach evaluation form

Name:	
Date of completion	

	Question	Details
1	Date DPO notified	
2	Breach type?	Choose from: ☐ *Loss* ☐ *Unauthorised disclosure* ☐ *Unauthorised access* ☐ *Deliberate action/inaction* ☐ *Released data to incorrect person* ☐ *Devices lost* ☐ *Theft* ☐ *Alteration of data without permission* ☐ *Loss of availability of data e.g. Ransomware;* ☐ *Inaccurate data*
3	What is the personal data?	
4	When were you first aware of this issue?	
5	How did the breach occur?	
6	Where is the data now?	
7	Who might have access to the data?	
8	What should have happened?	
9	Are there any processes / policies that should have been adhered to?	
10	What is being/has been done to deal with the breach?	

Return this form to the DPO: Enquiries@scottishlegalcomplaints.org.uk

scottish legal complaints commission slcc

Data breach assessment form

Name:	
Date of completion	

	Question	Details
1	Are we still within 72 hours?	
2	Is the data 'special category'?	
3	Are the individuals affected identifiable?	
4	Is there a discernible risk to the rights and freedoms of any individuals e.g. • Discrimination • Reputation • Financial loss • Confidentiality • Security • Economic or social disadvantage	
5	Is a report required to the affected persons?	
6	Is a report to the ICO required?	
7	Have we got all evidence/ responses required?	
8	Are we in a position to provide the ICO with all the necessary information?	
9	Has this happened before?	
10	Are there any further steps required in connection with this specific breach (not training/ lessons learned etc)?	

Guide to assessing the severity of the breach incident

The purpose of this guidance is to support the DBRT in its assessment of data breach incidents which may or may not be required to be reported to the ICO.

Factors – scale	Factors – sensitivity
Numbers of individual data subjects affected (if unknown, worse case scenario should be applied)	Potential for media interest Potential for reputational damage Potential litigation Significant distress or damage to data subject(s)

STEP 1 - establish the **scale** of the incident (estimate the maximum potential scale point)	Baseline scale point	No. of potential data subjects affected
	0	Less than 11
	1	About 11-50
	1	About 51-100
	2	About 101-300
	2	About 301-500
	3	Over 501

STEP 2 - identify which **sensitivity** characteristics may apply and adjust the baseline scale point accordingly		
Sensitivity Factors		
Low: for each of the following factors, reduce the baseline score by 1	Risk	Notes
-1	No 'Special Category' personal data at risk or data to which confidentiality is owed	*e.g. Racial, religious, ethnic, mental health, sexual preference etc*
-1	Data is readily accessible or already in the public domain (or would be made available under FOISA)	
-1	Data unlikely to identify any individual(s)	*e.g. Demographic data such as lists of postcodes etc*
High: for each of the following factors, increase the baseline score by 1	Risk	Notes

	+1	Detailed information at risk	*e.g. Investigation or determination reports, complaint form*
	+1	High risk confidential information	*e.g. Children's data; criminal offence data; data protected by other statutory requirement or court order*
	+1	One or more previous incidents of same / similar type in past 12 months	*e.g. More than one incident where an email containing special category data or confidential data identifying a living individual has been sent to the wrong person. Could include multiple incidents within a specific team/dept.*
	+1	Failure to implement, enforce or follow organisational / technical safeguards to protect the information	*e.g. Data has been transferred onto an unencrypted USB in breach of organisational policy and has been lost.*
	+1	Likely to attract media interest and / or a complaint has already been made to ICO be a member of the public, other organisation or individual	*e.g. Loss of large volumes of personal identifiable data, disclosure of information relating to sex offenders / criminal data / vulnerable adults. ICO is duty bound to investigate if report made, so would attract more attention*
	+1	Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment to their rights / freedoms	*e.g. Financial loss, fraud, significant level of upset, emotional or mental pain (going beyond annoyance or irritation), details of individual whose ID should be protected*
	+1	Individuals affected are likely to have been placed or may be placed at risk of or incurred physical harm	*e.g. details of individual whose ID should be protected, refuge houses etc*

STEP 3 - Categorisation	Level	Action
	0 or 1	Logged by DPO, but no need to report to ICO; potential notification to data subjects affected (if appropriate)

	2 or 3 (or more)	Must be automatically reported to the ICO
	The “near miss”	Where there hasn’t been an incident or severity is reduced due to fortunate events (rather than pre-planned controls), report to DPO for learned activities and logging

Assessment Outcome:

scottish legal complaints commission slcc

Data breach follow up form

Name:	
Date of completion	

	Question	Details
1	Outcome of specific breach?	
2	Remedial action taken in connection with specific breach?	
3	What training has historically been provided to prevent this action?	
4	What awareness-raising measures have been taken since this breach?	
5	What feedback has been received from the Data Controller?	
6	What feedback has been received from the ICO?	
7	What action is now required to prevent this from occurring again?	
8	Has a meeting been set up with the appropriate person(s) to discuss the breach?	

Appendix 5 - Document Control Information

Original Author:	SLCC	
Date:	24.05.18	
Last Major Version Approved by:	New	
Original Major Version Approval Date:	24.05.18	
Document name, version and location:	G:\Policies and Procedures\Communications\COM015 Data Breach Policy & Process v01.00 2018.05	
Number of pages:	18	
Review Date:	12.2018	
Published:	**Yes~~/no~~**	**Date: 24.05.2018**

Record of Document Changes

Date	Version no. changed	New version no.	Brief Description of change and reason	Changed by	Authorised by
24.05.18	-----	v01.00	New policy and process created (to replace COM013 v01.02– following GDPR)	AM	CEO