Guidance on whether to notify the ICO of a loss of personal information.

Overview

This document provides guidance to Hampshire Constabulary and Thames Valley Police on a decision making process for notifying the Information Commissioner's Office (ICO) in the event of the loss, theft, unauthorised disclosure or compromise of personal information. This decision will be referred to and made by either the Senior Information Risk Owner (SIRO) or the Head of the Joint Information Management Unit (JIMU) and will be one of the many activities that will take place in the wider management and investigation of a data loss.

'Personal information' is information which can identify a living individual. This can include information that, when combined with other readily available data, can identify a living individual.

If a loss, theft, unauthorised disclosure or compromise of non-personal data occurs then it will not be necessary to consider whether or not to notify the ICO.

Legal Requirements

The use of personal information is governed by the principles set out in the Data Protection Act 1998. Under the Act all data controllers have a responsibility to ensure appropriate and proportionate security of the personal data they hold by taking 'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

Although there is currently no legal obligation on forces to report breaches of security which result in the loss, theft, unauthorised disclosure or compromise of personal data, the Information Commissioner believes 'serious' breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered by the ICO together with whether the force is properly meeting their responsibilities under the Act. The ICO will also advise the force, if asked, on how to manage and minimise the impact of the loss on the data subject.

Any individual who becomes aware of the loss of their own or someone else's personal data can make a complaint directly to the Information Commissioner. Any such complaint will normally trigger an investigation by the ICO. Whether or not the incident had already been reported by the organisation involved would normally be considered by the investigators and the subsequent judgement.

‘Serious’ breaches are not defined by the ICO. However; the ICO Guidance advises that the following criteria should be the main factors in considering whether breaches should be reported:

- The potential detriment to individuals (the overriding consideration).
- The volume of personal data lost / released / compromised.
- The sensitivity of the data lost / released / compromised.

The following guidance provides a framework for assessing whether the ICO should be informed.

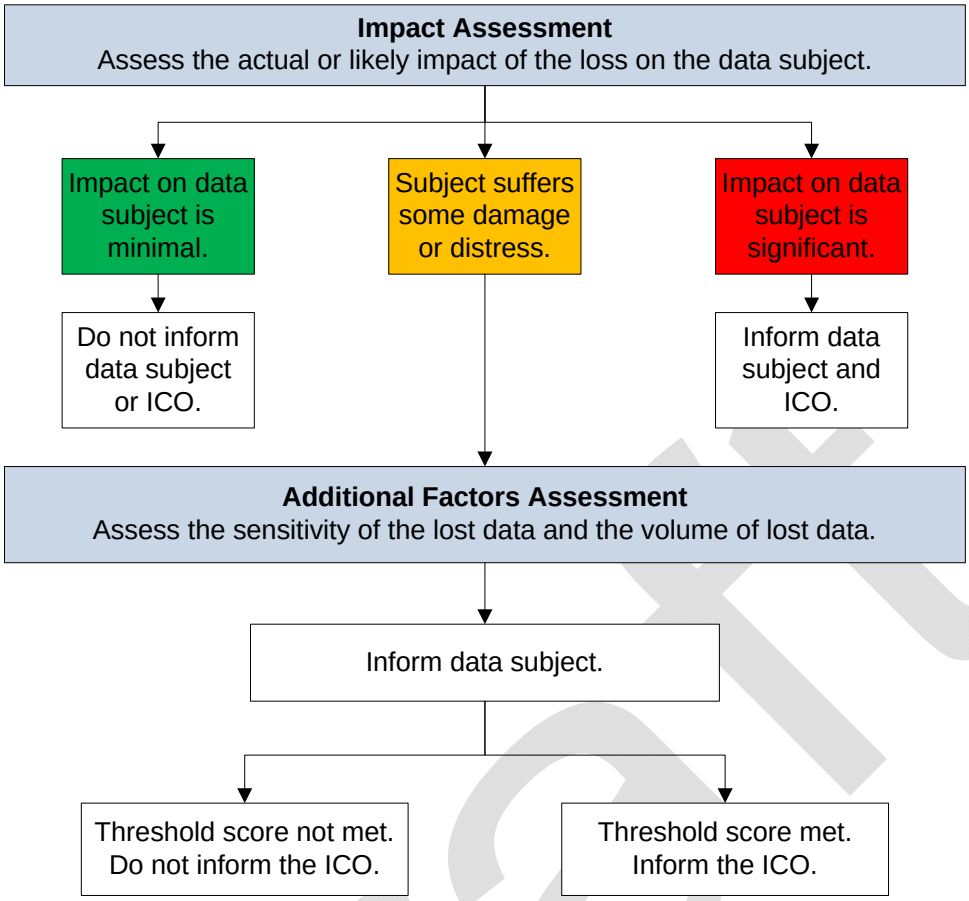
Notification Matrix:

The Notification Matrix on the following pages will help to determine whether a loss, theft, unauthorised disclosure or compromise of personal data is 'significant' and therefore should be reported to the ICO. Fundamental to this matrix is the use of the National Decision Model and that normal force policies such as Critical Incident investigation are not superseded by it, but that factors are considered in light of it.

The use of individual discretion is not prevented. Acting outside of this guidance is permitted where the decision can be justified and the rationale is recorded in sufficient detail. Examples of circumstances where the use of discretion may be considered are where the loss is a repeated incident or where there is significant impact on public confidence. Adherence to the Code of Ethics may facilitate making discretionary decisions of the highest professional standards of public service.

Whilst the model below is purely referring to the data subject and ICO notification, it is expected to operate within, and therefore also be assessed within the operational context of any related / directly connected incident. This will ensure that the primary concern of public safety is always paramount.

The rationale and outcome of notification decisions should be recorded by JIMU as part of the incident record within the ‘Information Security Incident Spreadsheet’.



When using the Notification Matrix to assess all three of the above assessment factors (**impact, sensitivity and volume**) it is not necessary to satisfy all the criteria in a particular box. A 'best fit' approach is advised.

Timing Of Any Notification

If the outcome is to notify the ICO of the data protection breach, consideration must be given as to when to notify. Ordinarily notification should occur as soon as the information required in the ICO's Notification Form is available (further information about what is required is listed in Appendix A). However; consideration must be given as to whether notifying the ICO could prejudice an ongoing investigation or operation and if so it may need to be delayed.

Where the breach is a critical incident and a Gold Group has formed, the timing of ICO notification will be a matter for their consideration and discussed with the SIRO or Head of JIMU. Where the matter is not a critical incident, the Head of JIMU will liaise with a senior manager of the relevant business area to establish whether a delay is required and will inform the SIRO. The Head of JIMU will also make the Head of Corporate Communications aware of any subsequent decision to notify the ICO.

The Head of JIMU will report the breach to the ICO. In their absence this will be delegated to a member of the JIMU Senior Management Team.

Notification Matrix - Impact Assessment:

Criteria	Severity			
Impact on data subject (actual or likely)	- Minimal level of data exposure (e.g. data unlikely to be exposed in the public domain, data sent in error to only a few trusted recipients such a statutory partners, or data sent to an individual with no intent to harm or publish). - Data fully recovered with no further exposure. - Access to data unlikely or deemed very difficult due to encryption or security protection. - **No detrimental impact to the data subject.**	- Low level of data exposure (e.g. exposed to limited number of people who either know or know of the subject). - Subject may suffer damage or distress. - Subject may suffer embarrassment or reputational or financial damage. - Subject is vulnerable.	- Wider level of data exposure (e.g. in local or regional media, or posted on an open source website). - Subject may become victim of crime. - Subject may suffer: identity theft, financial loss. - Subject may suffer: threat to safety or threat of harm. - Subject is vulnerable. - May cause significant impact on subject's livelihood, employment or reputation.	- Broad level of data exposure (e.g. in national media). - May result in risk of serious harm or threat to life. - May result in serious injury or death. - ICO advice is needed to manage and reduce the impact of the loss, on the subject.
	Data subject does not need to be informed of the data loss. ICO does not need to be notified unless the volume of data lost is significant (over 1000 data subjects).	Data subject should be informed of the data loss. Data loss should be reported to the ICO if the additional 'volume' and 'sensitivity' severity scores total 4 or more.	Data subject should be informed of the data loss. Data loss should be reported to the ICO if the additional 'volume' and 'sensitivity' severity scores total 3 or more.	Data subject must be informed of the data loss. Data loss must be reported to the ICO.

Notification Matrix - Additional Factors Assessment:

If **impact assessment = green** or **red**: no requirement to assess the below **'sensitivity'** or **'volume'** of lost data. Follow the notification guidance above.

If **impact assessment = amber**: assess the **'sensitivity** of lost data' and **'volume** of lost data' by using the below table. For both factors identify the appropriate level of severity to provide a score for each factor.

Sensitivity of data	- Personal information. - Subject matter or the nature of the event already easily accessible in the public domain (e.g. publicised arrest). - GPMS – Protect - GSC – Official	- Sensitive personal data (e.g. offending, convictions, health / medical, safeguarding, ethnicity). - Financial information. - Information that the 'public' would consider as sensitive. - GPMS – Restricted - GSC Official Sensitive	- Very sensitive personal information (e.g. relating to serious / organised crime, sex offenders, sensitive safeguarding matters, high risk PVP, Handling Code 4 intelligence). - GPMS Confidential - GSC Official Sensitive	- Highly sensitive personal information (e.g. Covert Human Intelligence Source, witness protection, intelligence with a handling code of 5). - GPMS Secret - GSC Secret / Top Secret
	Severity score = 1	Severity score = 2	Severity score = 3	Severity score = 4
Volume of data	1- 5 data subjects (including any non police officer 3rd parties mentioned).	6 -100 data subjects (including any non police officer 3rd parties mentioned).	101 - 1000 data subjects (including any non police officer 3rd parties mentioned).	More than 1000 data subjects (including any non police officer 3rd parties mentioned).
	Severity score = 1	Severity score = 2	Severity score = 3	Severity score = 4

Add the **sensitivity + volume** scores and then return to the **amber** '**Impact Assessment'** boxes' to determine if notification is required.

What Could Happen As A Result Of Notifying The Information Commissioner:

The Information Commissioner will:

- Record the breach
- If asked, offer advice on managing and minimising the impact of the loss on the data subject.
- Decide whether to take further investigative action by assessing the seriousness of the breach and the adequacy of any remedial action taken, to determine a course of action. The investigation could lead to one of the following courses of action:
    - Take no further action.
    - A requirement on the force to undertake a course of action to prevent further breaches.
    - Formal enforcement action turning such a requirement into a legal obligation.
    - Where there is evidence of a serious breach of the DPA, whether deliberate or negligent, the serving of a monetary penalty notice requiring the organisation to pay a monetary penalty of an amount determined by the Commissioner up to the value of £500,000.

It is not the Information Commissioner's responsibility to publicise security breaches not already in the public domain or to inform any individuals affected. In so far as they arise, these are the responsibilities of the force. However, the ICO may recommend that the data controller make a breach public where it is clearly in the interests of the individuals concerned or if there is a strong public interest argument to do so.

Further Guidance:

1) Further guidance on investigating and notifying a security breach or information loss is available from the Information Commissioner's website by using the below link:

   Information Commissioner's Office - what should I do if I lose personal data.

2) Further guidance on data loss management is also available from the ACPO Data Protection Manual of Guidance Part 1 (chapter 13)

3) Joint Information Management Unit Help Desk:

   Hampshire: information.management@hampshire.pnn.police.uk
   Tel: 01962 871541 (internal 79 2128)

   Thames Valley: information.management@thamesvalley.pnn.police.uk
   Tel: 01865 846329 (internal 700 6329)

Appendix A: Information Needed To Notify A Breach To the ICO

Once authorised, the breach will be reported to the ICO by the Head of JIMU or a member of the JIMU Senior Management Team in their absence. Listed below is the information required, by the ICO, to report the breach. All criteria marked with (*) are mandatory.

1. **Organisation details**
   - * Name of organisation and whether it is the data controller in respect of this breach? (Supply data controller's registration number).
   - * Contact details (if further details are required concerning the incident)?

2. **Details of the data protection breach**
   - * Description of the incident including how and when it happened.
   - If reporting the incident to the ICO has been delayed, explain the reasons.
   - What measures were in place to prevent an incident of this nature occurring?
   - Provide extracts of any policies/procedures considered relevant to this incident (provide the dates on which they were implemented).

3. **Personal data placed at risk**
   - * What personal data has been placed at risk and to what extent? Specify if it includes any financial or 'sensitive personal' data.
   - * How many individuals have been affected?
   - * Are the affected individuals aware that the incident has occurred?
   - * What are the potential consequences and adverse effects on them?
   - Have any affected individuals complained to the organisation?

4. **Containment and recovery**
   - * Has the organisation taken any action to minimise/mitigate the effect on the affected individuals (provide details)?
   - * Has the data placed at risk now been recovered (provide details)?
   - What steps has your organisation taken to prevent a recurrence of this incident?

5. **Training and guidance**
   - Does the organisation provide its staff with data protection training (provide relevant extracts)?
   - Confirm if data protection training is mandatory for all staff. If so when had the staff members involved received training?
   - Does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting (provide extracts)?

6. **Previous contact with the ICO**
   - Have you reported any previous incidents to the ICO in the last two years?
   - If yes, provide: brief details, the date reported and, if known, the ICO urn).

7. **Miscellaneous**
   - Have you notified any other (overseas) data protection authorities (provide details)?
   - Have you informed any other regulatory bodies about this incident (provide details)?
   - Has there been any media coverage of the incident (provide details)?