Eurachem procedure in the event of 'personal data breach'

Introduction

Current EU regulations require that certain types of personal data breach are reported to the relevant supervisory authority as soon as possible and within 72 hours of becoming aware of the breach where feasible.

In addition, significant breaches of personal data need to be notified to individuals who may be affected, both as a matter of good practice and to comply with EU regulations.

This procedure sets out what actions Eurachem will take in the event of a personal data breach. It includes:

- The classes of event that constitute a personal data breach;
- How breaches are identified and reported to Eurachem;
- The responsible officers in the event of a breach;
- The general procedure to be followed in the event of a breach or suspected breach;
- The circumstances in which Eurachem will notify individuals, and the information to be provided to individuals;
- Classes of event that Eurachem considers as breaches notifiable to the competent authority under the General Data Protection regulation;
- The relevant competent authority for most breaches;

Scope

This procedure is applicable to data breaches involving all classes of personal information held by Eurachem Officers and Eurachem Working Groups.

This procedure should be read in conjunction with the Eurachem Policy on use of Personally Identifiable Information.

What is a Personal data breach?

General

A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Note: A breach is more than just about losing personal data; it includes any kind of inappropriate disclosure to a third party (malicious or otherwise), and events that may result in such disclosure.

Examples

Examples of personal data breach include:

- Loss of equipment (USB device, laptop, CD-ROM, tablet compute) that holds personal information in the control of Eurachem, whether or not the personal data has been, or can be, accessed;
- Sending personal data to an incorrect recipient;
- Unauthorised access to a system (such as the Eurachem Website, the file system used by the Eurachem Secretariat, or file systems used by Working groups) that holds unpublished personal information, whether or not there is evidence that personal data has been accessed;
- Permanent or extended* loss of access to essential personal information.

*Temporary loss of access due to brief system outages, maintenance etc. are not considered as los of access for this purpose.

Identification of personal data breaches

A personal data breach can be identified by:

- The officer responsible for the information or system holding personal information;
- A service provider (e.g. web host) or other organization (e.g. Secretariat's employer) that is responsible for a system holding personal information held by Eurachem.
- An individual whose data is held by Eurachem;
- A third party who becomes aware of a breach.

Reporting a personal data breach

1. Individuals and officers should report any breach or suspected breach without delay to
   - For breaches involving the Eurachem website:
     The Eurachem Webmaster (Website contact form:
     https://www.eurachem.org/index.php/contacts/cntweb) or email
     webmaster@eurachem.org, and advise or copy to the Eurachem Secretary (below)
   - All other breaches: The Eurachem Secretariat
     (Website contact form: https://eurachem.org/index.php/contacts) or email
     secretariat@eurachem.org.
2. Eurachem officers receiving a report of a breach from a service provider or third party should advise the Secretariat or Webmaster as above.

Eurachem officer responsibilities

Coordination of response:

Breaches involving the Eurachem website: The Eurachem Webmaster

All other breaches: The Eurachem Secretary

Decisions on risk to individuals and appropriate level of response

The current Chair and Vice chairs (or those available within 24h of the breach) are responsible for deciding whether a breach is notifiable to the competent authority, and for agreeing proposed action, remediation and follow up.

General procedure

On identification of a personal data breach or suspected breach:

1. The officer responsible for coordinating response will advise the Chair and Vice Chairs ("the Chairs") of the incident;
2. In consultation with available IT experts (including the Eurachem Webmaster, local experts etc. as available), the officer responsible will take any immediate technical or organisational measures necessary to minimize impact of the breach or suspected breach. This may include, for example:
   - Implementing temporary restrictions on access to systems;
   - Immediate change of passwords;
   - Reporting loss or theft of equipment to local law enforcement.
   - Where the risk to an individual appears high, immediate advice to the individual(s) affected.
3. The officer responsible will conduct a risk assessment (Annex 1) and advise the Chair and Vice Chairs of the outcome and recommended action within 24h of becoming aware of the breach;
4. The Chair and Vice Chairs will direct the responsible officer to act as the Chairs think necessary, taking account of the risk assessment, the particular circumstances, the risk to individuals affected, and applicable EU and national regulations.
5. The initial report, initial action taken, risk assessment, the Chairs' decision and the follow up action shall be documented in an incident report. This shall be provided to the Executive Committee and included in the minutes of the next Executive committee meeting, thereby forming a permanent record.

Specific action for different risk levels

After conducting the assessment in Annex 1, the following actions should normally be taken:

Class 0: No personal data breach

Remedial action to rectify fault; amend procedures or retrain staff to prevent recurrence. Notify Chairs and (in due course) Executive that the breach does not involve personal data.

Class 1: Personal data is all in the public domain

a) Notify Executive of personal data breach as per general procedure.
b) Take remedial action to rectify fault; amend procedures or retrain staff to prevent recurrence.

Class 2: Personal data is not public but is not high risk and is protected against disclosure

Breach is unlikely to result in risk to individuals’ rights and freedoms.

a) Advise affected individuals of the breach and provide information about the level of protection of the information so that individuals can decide whether action is needed for their own circumstances. [Note: this exceeds the GDPR requirement for individual notification]
b) Notify Executive of personal data breach as per general procedure.
c) Take remedial action to rectify fault; amend procedures or retrain staff to prevent recurrence.

Class 3: Personal data is not public, is not high risk, but is not protected against disclosure

Breach is unlikely to result in risk to individuals' rights and freedoms.

a) Notify Executive of personal data breach as per general procedure.
b) Advise affected individuals of the breach and warn individuals specifically that the information is not protected against unauthorized access.
c) Advise individuals to notify employer (if applicable) and follow employer's organizational procedures. [Note: this exceeds the GDPR requirement for individual notification]
d) Take remedial action to rectify fault; amend procedures or retrain staff to prevent recurrence.

Class 4: Sensitive or high risk personal information may have been compromised.

Breach could reasonably result in risk to individuals' rights and freedoms. Action must include:

a) Notify Executive of personal data breach as per general procedure.
b) Notify relevant competent authority/ies following the competent authority's guidance;
c) Notify individuals that a breach has occurred and provide any information on steps that they can take to protect against consequences. This can include, for example:
   - Advice to notify the individuals' employer of the breach and to follow any guidance provided by the employer;
   - Advice to change passwords, where password information is compromised;
   - Advice to notify financial institutions, in the (rare) event that financially sensitive information is held.
d) Take remedial action to rectify breach; Amend procedures or retrain staff to prevent recurrence;

Relevant competent authority

For most breaches, the relevant competent authority in the first instance ('lead' competent authority under the GDPR) will the national authority for the Secretariat's normal place of business. Any reports should be referred there in the first instance.

Additional information

The Article 29 Working Party has released guidance on the need for notification of personal data breaches; see Annex VII of

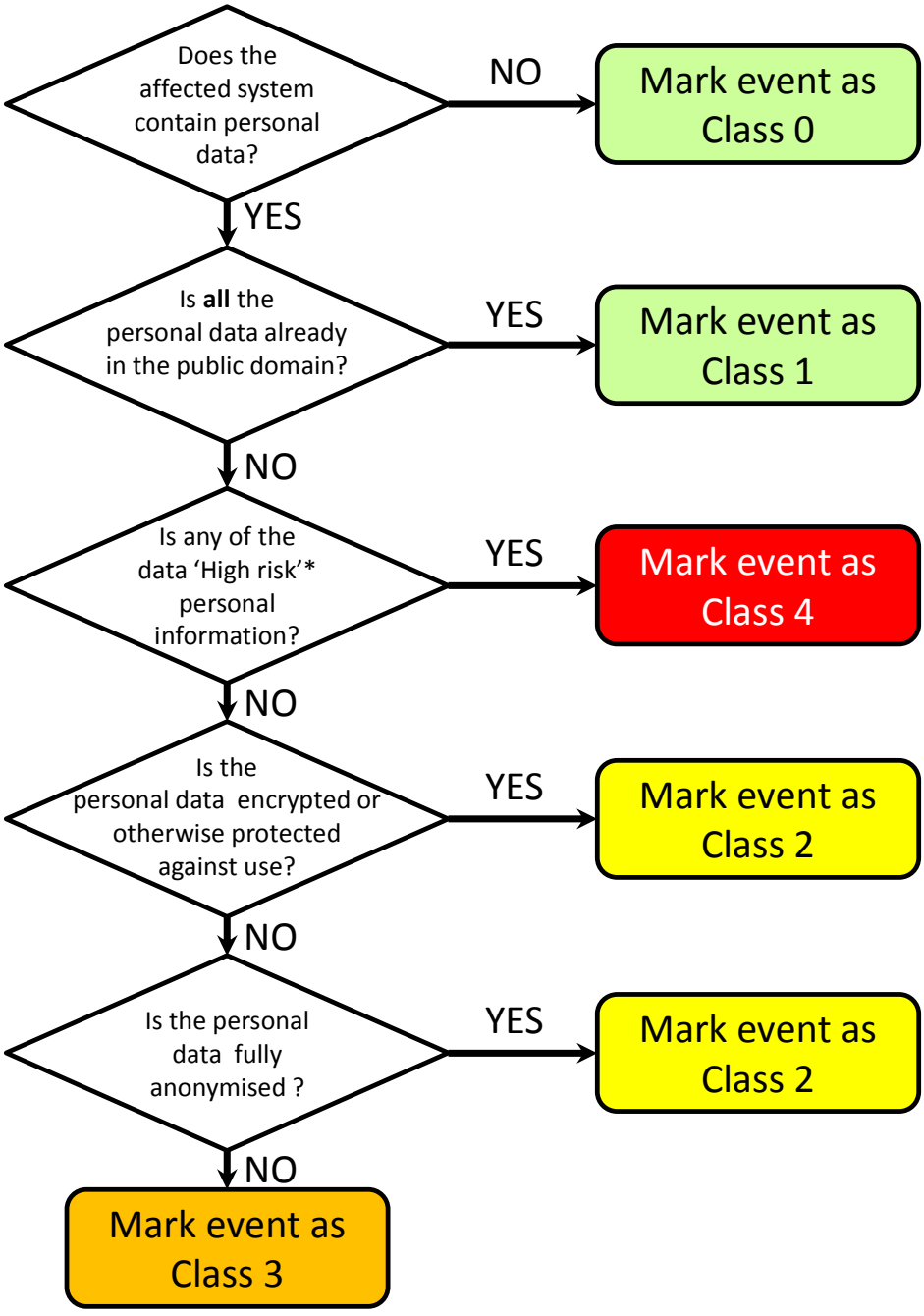
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

The risk assessment at Annex 1 is a simplified implementation of the guidance. In case of doubt, follow Article 29 guidance as updated from time to time.

Last updated:

Date	Nature of amendment
2019-09-13	Policy approved by Eurachem Executive.

Annex 1: Risk assessment for Eurachem personal data breach



*For this assessment, 'High Risk' includes

- 'Sensitive' personal information: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation
- Information allowing access to a person's finances
- Passwords or other information that may compromise other systems (e.g. password information, security questions);
- Any other information that could materially affects the rights, safety or privacy of an individual