European Liver Transplant Registry

Data Breach Protocol

Contents

1. Data breach and purpose of protocol

1.1. European Liver Transplant Registry (ELTR) has developed this personal data breach protocol as part of our strategic planning to ensure that ELTR is prepared to respond in a personal data breach situation. The focus of any breach response plan will be on prompt action to protect individuals and their personal data. ELTR is committed to:

(a) notifying the Data Protection Commission "Commission Nationale de l'Informatique et des Libertés" (CNIL) of a personal data breach without undue delay and not later than 72 hours after becoming aware of it (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).
(b) notifying affected data providers without undue delay unless the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons.

1.2. This protocol will be:

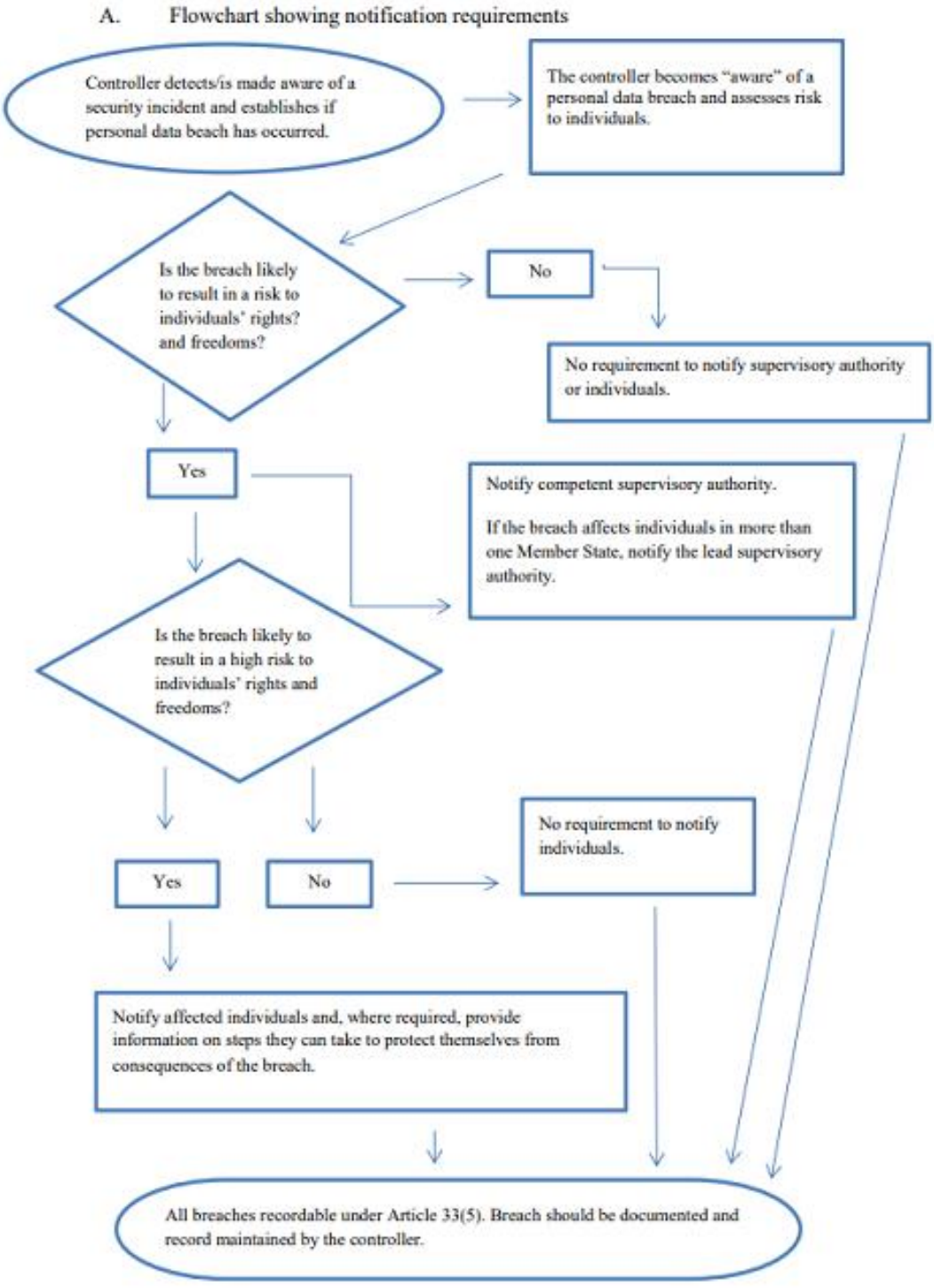
(a) circulated to all appropriate data processors. Data processors are required to alert ELTR immediately if the processor becomes aware of a breach of the personal data it is processing on behalf of ELTR
(b) advised to staff at induction and at periodic staff meetings/training.

1.3. The flow-chart overleaf (taken from the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017) summarises the steps to be taken:

1.4. Definitions:
In this protocol, the following terms shall have the following meanings[1]:

1.4.1. "**Aware**": a data controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
1.4.2. "**Damage**": the personal data has been altered, corrupted, or is no longer complete.
1.4.3. "**Destruction**": the data no longer exist or no longer exist in a form that is of any use to the controller.
1.4.4. "**Loss**": the data may still exist, but the controller has lost control or access to the data, or no longer has the data in its possession.
1.4.5. "**Personal data breach**": per Article 4(12) GDPR: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"·
1.4.6. "**Temporary loss of data**": an incident resulting in personal data being made unavailable for a period of time.
1.4.7. "**Unauthorised or unlawful processing**" may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

[1] Definitions taken from GDPR and WP250 ("Guidelines on Personal data breach notification under Regulation 2016/679).



1.5. A data security breach can happen for several reasons, including:

- Human error
- Loss or theft of paperwork, or any device containing data
- Break-ins, burglary, mugging
- Inappropriate access controls allowing unauthorised use/access
- Equipment failure and inadequate system back-ups
- A disaster such as flood or fire
- Phishing or blagging (where information is obtained by deception or spoofing)
- Malicious attacks such as hacking or ransomware attack

1.6. Personal data breaches can result in adverse effects on individuals which can result in physical, material, or non-material damage. This could include causing the data subject embarrassment, distress, or humiliation. Other adverse effect could include: *"loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, significant economic or social disadvantage*" to affected individuals (WP250 rev.01).

1.7. Personal data breaches can also be damaging to ELTR as they can result in:

• Damage to the relationship of trust we have built with our data providers and liver transplant community,
• Loss of, deletion of, or damage to personal data, which is essential to the administration of ELTR,
• Damage to the reputation of ELTR,
• Administrative fines in accordance with the provisions of Data Protection legislation, enforcement action, and/or litigation.

2. Protocol

In case of a personal data breach, ELTR will follow the following protocol:

2.1. Identify that there is an issue and alert the relevant people

2.1.1. The ELTR DPO shall be notified as soon as possible.
2.1.2. The ELTR DPO shall notify the General Manager, the ELTR Biostatistician and the IT provider/hosting company as soon as possible.

Emergency contact: Vincent Karam, PhD. (DPO)
Tel: (33) 145593437
Email: vincent.karam-ext@aphp.fr

2.1.3. The ELTR DPO shall gather the ELTR team to assess the potential exposure/loss and undertake appropriate containment/mitigation/remediation measures.
2.1.4. The ELTR DPO shall start a written chronology of events, recording all relevant matters, including:
   (a) Date and time of notification of the breach (using the format DD/MM/YYYY and am/pm as appropriate).
   (b) If the notification relates to a potential breach, details of any preliminary investigation (if required) in order to establish whether or not a breach has in fact occurred.
   (c) Details of who reported the matter.
   (d) Details of what was known/suspected at that initial stage.
   (e) Details of what system/dataset is involved.
   (f) Assessment of risk to the rights and freedoms of natural persons.
   (g) Immediate actions undertaken (investigation, containment, mitigation, recovery, etc).
   (h) Details of the team gathered to assist.
   (i) Details of the tasks allocated to each team member.
   (j) At the same time as (g), notification to CNIL within 72 hours after having become aware.
   (k) Notification to the affected center(s) or Organ Sharing Organization(s), if required, without undue delay

2.1.5. Regardless of whether (or not) a decision is made to notify the CNIL, all documentation relating to documenting a (potential/reported/suspected) personal data breach including but not limited to the documentation required by Article 33(5) GDPR shall be stored on ELTR's Risks Register.

2.2. Containment, mitigation, and recovery

2.2.1. ELTR will immediately seek to contain the matter (insofar as that is possible) and shall take all necessary steps to mitigate any further exposure of the personal data held.
2.2.2. Where the data breach relates to an IT system and/or electronic data, contact shall be immediately made with the data processor responsible for IT support in ELTR. Their advice and assistance should be sought in relation to appropriate measures of containment, quarantine, preservation of data and logs etc.
2.2.3. Depending on the nature of the breach/threat to the personal data, this may involve:
(a) a quarantine of some or all PCs, networks etc.
(b) directing staff not to access PCs, networks, devices etc.
(c) suspending accounts,
(d) audit of the records held on backup server/s,
(e) ascertain the nature of what personal data may potentially have been exposed.
2.2.4. Consider a quarantine of manual records storage area/s and other areas as may be appropriate.
2.2.5. In appropriate cases, immediate consideration should be given to retaining an IT forensics specialist and obtaining legal advice.

2.3. Assess Risk

2.3.1. ELTR shall undertake an assessment in relation to the risk: is the personal data breach likely to result in a risk to the rights and freedoms of natural persons?
2.3.2. Classification of that risk:
- No risk?
- Risk?
- High risk?

If it is assessed that there is "no risk", the reasons for that decision must be recorded.
2.3.3. When assessing risk, ELTR shall have due regard to the sensitivity of the data and the category of the data subject in order to ascertain whether they may be placed at greater risk because of the breach.
2.3.4. ELTR may not be required to notify the CNIL and data providers if the breach is unlikely to result in a risk to their rights and freedoms, e.g., the data were securely encrypted with state-of-the-art encryption, and the key was not compromised in any security breach.
2.3.5. ELTR shall have regard to the recommendations made by the European Union Agency for Network and Information Services (ENISA) for a methodology in assessing the severity of a breach.
2.3.6. If a decision is taken not to notify the CNIL and/or affected data providers, the justifications for that decision will be documented and stored on ELTR's Risks Register.

2.4. Notification

2.4.1. Reporting of incidents to the Data Protection Commissioner ("CNIL"): All incidents in which personal data and sensitive personal data has been put at risk shall be reported to the CNIL without undue delay and where feasible, not later than 72 hours after having become aware of it unless it does not result in a risk to the rights and freedoms of data subjects.

CNIL Contact details

Telephone:	+33 1 53 73 22 22
Notification address	https://notifications.cnil.fr/notifications/index
Address:	Le délégué à la protection des données à la CNIL 3 Place de Fontenoy TSA 80715 75334 PARIS CEDEX 07 - France

2.4.2. At a minimum, the initial notification to the CNIL shall contain the following:

- The nature of the personal data breach.
- The categories of data subjects (e.g., liver transplant patients).
- Approximate number of data subjects affected.
- Categories of personal data/records (e.g., health data).
- Approximate number of personal data records concerned.
- Name and contact details of the ELTR DPO (from where more information can be obtained).
- Description of the likely consequences of the personal data breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy etc).
- Description of the measures undertaken (or proposed to be undertaken) by ELTR to address the breach (including, where appropriate, measures to mitigate its possible adverse effects).
- Important note: where the exact details of any of the above are not yet known, this shall not delay a timely breach notification to the CNIL. Further information can follow, when available: "*the information may be provided in phases without undue further delay*" (Article 33(4) GDPR).

2.4.3 If the controller chooses to only notify the Data Protection Commission, it is recommended that the controller indicates, where appropriate, whether the breach involves establishments located in other Member States.

2.4.4 Purpose of CNIL notification:

(a) Avoid an administrative fine: Failure to notify the Data Protection Commission as required under the Data Protection Act 2018 may result in an administrative fine.

(b) Advice: so that ELTR can obtain advice from the CNIL, and to ensure that its decisions about notifying (or deciding not to notify) affected data providers can be justified.

2.4.5 Notifying affected data providers

Following the risk-assessment conducted at 2.3.1, if the personal data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, ELTR shall:

(a) Contact the individuals concerned (whether by phone/email etc) without undue delay.

(b) Advise that a data breach has occurred.

(c) Provide the data providers with the detail outlined at 2.4.2 above.

(d) Where appropriate, provide specific advice so that the data providers can protect themselves from possible adverse consequences of the breach (such as re-setting passwords).

2.4.6 The communication to the data subject shall not be required if any of the following conditions are met:

(a) ELTR has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) ELTR has taken subsequent measures which ensure that the high risk to the rights and freedoms of data providers is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data providers are informed in an equally effective manner.

2.5. If the notified violation is the result of a cyber-attack, a complaint should be filed at the nearest police station or gendarmerie and all technical evidence in your possession should be made available to the investigators.

2.6. Post-event: After the initial response measures have been addressed, a full review should be undertaken in a timely manner. These should include the following:

2.6.1 Review of the breach record per Article 33(5) - document maintained by ELTR in its Risk Register.

2.6.2 Details of learning outcomes, improvements, and safeguards should be identified.

2.6.3 ELTR shall receive an appropriate briefing from the CNIL DPO (and/or such other external experts as may be retained to assist), and a copy of any investigation reports and any correspondence exchanged with the CNIL and/or affected data providers.

2.6.4 ELTR will give careful consideration to whether disciplinary procedures should be initiated, if relevant.

2.6.5 Where remedial actions are necessary, responsibility shall be allocated to individual(s): they shall be allocated responsibility for ensuring certain actions are completed within defined timeframes.

2.6.6 Staff should be apprised of any changes to this protocol and of upgraded security measures. Staff should receive refresher training where necessary.

Appendix 1 - Data Security Breach – Incident report

CNIL Online Incident Report

CNIL Notification form (pdf)

Appendix 2 - Guidelines on Personal Data Breach Notification under Regulation 2016/679

https://ec.europa.eu/newsroom/article29/items/612052

Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber-attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.

iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.

vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross border processing.	Yes, as could lead to high risk.	The controller should take action, e.g., by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g., under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (The controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore, is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g., under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers, a notifiable breach may not have occurred, but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	

ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g., a mailing list of a psychotherapist) or if other factors present high risks (e.g., the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.