Data Breach Management Regulation

13/03/2024

Ref No. DP004

Document owner and approver(s)	
Owner	The International Institute for Justice and the Rule of Law (IIJ)
Approver(s)	Mr. Steven Hill (Data Controller) Mr. Reinhard Uhrig (Acting Data Controller)

Regulation Statement

The International Institute for Justice and the Rule of Law ("the IIJ") will investigate and provide notice of personal data breaches to affected individuals and/or the Information and Data Protection Commissioner (the "IDPC") in accordance with applicable EU and local legislation requirements.

This regulation defines the steps that personnel must follow to ensure that personal data breaches are identified, contained, investigated, and remedied. It also provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, it establishes responsibility and accountability for all steps in the process of addressing personal data breaches.

Scope

This regulation applies to all users of personal data processed by the IIJ, whether staff, contractors, consultants, or agents thereof. This regulation further applies to any computing or data storing devices owned or leased by the IIJ that experience a data breach, as well as any computing or data storing device, regardless of ownership, which is used to store personal data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of personal data.

Definitions

Notification: the act of informing the competent authorities and, when required, persons affected by a personal data breach

Personal Data includes, without limitation, personally identifiable information (PII), and special category data.

- *Personally Identifiable Information (PII)* information relates to an identified or identifiable natural person ('data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- *Special Category Data* – includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Such incidents may be caused, among others, by:

- Accidental loss
- Theft
- Human error e.g. email containing personal data sent to the wrong person.
- Equipment failure
- Damage e.g. fire, flood
- Malicious activity e.g. hacking.

Procedure

If a personal data breach occurs, the IIJ will respond to and manage the breach effectively by means of a 5-part process:

1. Reporting a Breach
2. Containment and Recovery
3. Assessing the Risks
4. Notification of Breaches
5. Evaluation and Response

The IIJ shall appoint a Data Breach Team, comprised of at least six members, which shall include the Data Protection Officer, the Data Controller, and other members from different departments. The current members of the Data Breach Team are the following:

Steven Hill – Executive Secretary (Data Controller)

Reinhard Uhrig – Director Administration & Outreach (Acting Data Controller)

Karl Dimech – Administrative Officer (Data Protection Officer)

Quentin Balthazart – Monitoring and Evaluation Manager

Ali Khair – Outreach and Communications Manager

Kyra Busuttil – Human Resources Officer

The Data Breach Team shall be responsible for the overall implementation of this regulation.

1. **Reporting a Breach**

Article 33 of GDPR requires the IIJ to report a data breach to the Office of the Information and Data Protection Commissioner within 72 hours of it being discovered.

In some cases, the IDPC should also be informed of suspected breaches, if significant.

It is therefore critical that once any member of staff or authorized third party has knowledge of a breach, or suspects that a breach has occurred, they must contact the Data Protection Officer immediately.

All known details should be included in the initial reporting of the incident, including:

- staff contact information
- Name(s) of staff member(s) involved
- A brief description of what happened
- A general description of the personal data affected

The Breach Team shall log the incident, and initiate evaluation.

The evaluation process shall include:

a. Securing the data,
b. Preserving evidence,
c. Informing the Director (Head Of Department) concerned;
d. Contacting the IDPC, if appropriate and providing a preliminary notice of the suspected Security Incident; and
e. Establishing the scope of the Incident.

Confirmation of a breach having occurred will activate an official record of the circumstances leading to the breach, managing the data loss, individuals involved and evaluation/recommendations.

2. Containment and Recovery

Once details of the breach are known, the Breach Team will liaise with relevant personnel to contain the effect of the breach. This may include personnel from various departments and external suppliers of ICT and Communications. The Breach Team and the appointed specialists will agree what action must be taken to limit the damage caused by the breach and if possible, restore any lost data. Priority actions may include password changes.

3. Assessing the Risks

Once the breach has been contained, the Breach Team will assess the risks associated with the loss of data.

Considerations will be given to the following:

- Type of data e.g. hardcopy, electronic, personal data, sensitive data
- Nature of the loss e.g. theft, damage
- Has the data been encrypted
- What information does the data provide to an authorised party who may now have access
- How many individuals are potentially affected by this loss
- What categories of individuals are affected e.g. staff, suppliers,clients
- What threat may be posed to those individuals e.g. financial loss, contract details

4. Notification of Breaches

If the personal data breach is unlikely to result in risk to the rights of the data subjects, there is no obligation to report to the IDPC.

Notifying the Information and Data Protection Commissioners Office (IDPC)

The IDPC must be notified of all breaches where large numbers of individuals are involved or where the consequences are serious, and this within 72 hours of discovery of the breach.

The Data Protection Officer will be responsible for such notification.

As per Article 33.2 of GDPR, when notifying the IDPC, the information should include, at a minimum:

- nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- name and contact details of contact person from where further information can be obtained.
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The IDPC will not normally inform the media of a breach however they may advise the IIJ to inform the media of the breach.

Notifying the Media

Should the IDPC advise that the media is to be informed of the data breach, the Breach Team will liaise with the Communications and Outeach Department to agree on a statement which will be released, containing all relevant information pertaining to the incident.

Notifying the individuals

Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects, the IIJ is obliged to notify all parties affected by the breach without undue delay.

The Breach Team will establish the identities of individuals whose personal data have been compromised and formulate the correspondence to be sent to each subject.

The correspondence should inform the data subjects that their information was included in the breach and the steps they can take to protect themselves and their privacy. Notification to affected individuals will be overseen by the Breach Team, and is to include the following information:

1. a general description in clear and plain language of the nature of the personal data breach and the type of personal information affected;

2. the name and contact details of the contact point where more information can be obtained;
3. a description of the likely consequences of the personal data breach;
4. a general description of the steps the IIJ will take to protect the information from further unauthorized access or acquisition and measures to mitigate any possible adverse effects;

5. Evaluation and Response

While it is critical to contain and assess the risks of a breach, the IIJ must evaluate events leading to the breach and the effectiveness of its response to it. While carrying out an evaluation, the Breach Team will convene with department heads and if necessary seek legal advice or advice from the IDPC regarding what measures the IIJ should and can take to avoid a breach of a similar nature in future.

Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures
- Was the breach a result of inappropriate training
- Where are documents stored
- Who has access rights to what data
- Has this breach identified potential weaknesses in other areas
- Security of electronic information assets

<u>IDPC Response</u>

The IDPC will evaluate the data breach and carry out their own investigation into the surrounding circumstances, the nature and seriousness of the breach, and the adequacy of any remedial action taken by the IIJ will be assessed and a course of action determined. Depending on the seriousness of the breach, the IDPC may also impose administrative penalties.

Documentation

The Data Breach Team will document all reported data security breaches. Documentation responsibilities include:

- Log of incidents received.
- The evaluation process and outcome of the evaluation.
- Recommended corrective action to contain the incident and prevent future incidents.
- Breach determination outcome.
- Identification of Responsible Department.

- Documentation of notice made to affected individuals, business associates, and the IDPC where applicable.

Communication Plan

This procedure will be communicated to all members of staff.

Review

This procedure will be reviewed and or amended if required annually or sooner to reflect changes in legislation or other circumstance.

How to Contact Us

Full Name	**Primary Number**	**Secondary Number**
Steven Hill	+35699314795	+1 917 318 0206
Reinhard Uhrig Karl Dimech	+35699703044 +356 9908 1949	+43 6604 714 916