DATA BREACH RESPONSE AND NOTIFICATION PROCEDURE

Version:	1.0
Date of version:	March 2018
Created by:	Simeon Drage
Approved by:	Stephen Clapp
Confidentiality level:	External Use

Change history

Date	Version	Created by	Description of change
March 2018	1.0	Simeon Drage	Created document

Table of contents

1. Scope, purpose and users

This Procedure provides general principles and approach model to respond to, and mitigate breaches of personal data (a "personal data breach") in one or both of the following circumstances:

- The personal data identifies data subjects who are residents of the Member States of the European Union (EU) and countries in the European Economic Area (EEA), regardless of where that data is subject to processing globally; and
- The personal data is subject to processing in the EU and/or EEA, regardless of the country of residency of the data subject.

The Procedure lays out the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR.

All Employees/Staff, contractors or temporary Employees/Staff and third parties working for or acting on behalf of IRIS Connect ("Company") must be aware of, and follow this Procedure in the event of a personal data breach.

2. Reference documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Personal Data Protection Policy

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation (GDPR):

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 Regulation.

"Controller" is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation,

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Personal Data Breach" means 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.

"Supervisory Authority" means an independent public authority which is established by a Member State pursuant to Article 51.

4. Data Breach Response Team

A Data Breach Response Team must be a multi-disciplinary team comprised of knowledgeable and skilled individuals in IT Department, IT Security, Legal, Legal and Public Affairs The team may be a physical (local) or virtual (multiple locations) team which responds to any suspected/alleged personal data breach.

The Financial Director appoints the members of the Data Breach Response Team. The Team must be appointed regardless of whether or not a breach has occurred.

The team must ensure that necessary readiness for a personal data breach response exists, along with the needed resources and preparation (such as call lists, substitution of key roles, desktop exercises, plus required review of company policies, procedures and practices).

The team's mission is to provide an immediate, effective, and skilful response to any suspected/alleged or actual personal data breaches affecting the Company.

If required, the team members may also involve external parties (e.g. an information security vendor for carrying out digital forensics tasks or an external communications agency for assisting the Company in crisis communications needs.

The Data Breach Response Team Leader can choose to add additional personnel to the team for the purposes of dealing with a specific personal data breach.

The Data Breach Response Team may deal with more than one suspected/alleged or actual personal data breach at a time. Although the core team may be the same for each suspected/alleged or actual personal data breach, there is no requirement for this.

The Data Breach Response Team must be prepared to respond to a suspected/alleged or actual personal data breach 24/7, year-round. Therefore, the contact details for each member of the Data Breach Response Team, including personal contact details, shall be stored in a central location, and shall be used to assemble the team whenever notification of a suspected/alleged or actual personal data breach is received.

5. Data Breach Response Team duties

Once a personal data breach is reported to the Data Breach Response team leader, the team must implement the following:

- Validate/triage the personal data breach
- Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded
- Identify remediation requirements and track resolution
- Report findings to the top management
- Coordinate with appropriate authorities as needed
- Coordinate internal and external communications
- Ensure that impacted data subjects are properly notified, if necessary

The Data Breach Response Team will convene for each reported (and alleged) personal data breach, and will be headed by the Data Breach Response Team Leader.

6. Data Breach Response process

The Data Breach Response Process is initiated when anyone who notices that a suspected/alleged or actual personal data breach occurs, and any member of the Data Breach Response team is notified. The team is responsible to determine if the breach should be considered a breach affecting personal data.

The Data Breach Team leader is responsible for documenting all decisions of the core team. Since these documents might be reviewed by the supervisory authorities, they need to be written very precisely and thoroughly to ensure traceability and accountability.

7. Personal data breach notification: Data processor to data controller

When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, the Data Protection Officer of the Company acting as a data processor must report any personal data breach to the respective data controller/controllers without undue delay.

The Data Protection Officer will send Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

DPO will record the data breach into the Data Breach Register.

8. Personal data breach notification: Data controller to supervisory authority

When the personal data breach or suspected data breach affects personal data that is being processed by the Company as a data controller, the following actions are performed by the Data Protection Officer:

1) The Company must establish whether the personal data breach should be reported to the Supervisory Authority.
2) In order to establish the risk to the rights and freedoms of the data subject affected, the Data Protection Officer must perform the Data Protection Impact Assessment on the processing activity affected by the data breach.
3) If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. However, the data breach should be recorded into the Data Breach Register.
4) The Supervisory Authority must be notified with undue delay but no later than in 72 hours, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.

DPO will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

9. Personal data breach notification: Data controller to data subject

The Financial Director must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject. If yes, the Data Protection Officer the Company must notify with undue delay the affected data subjects.

The Notification to the data subjects must be written in clear and plain language and must contain the same information listed in Section 7.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the Data Protection Officer must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

10. Accountability

Any individual who breaches this Procedure may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

11. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Call lists & substitution	Google drive of Data breach response team leader	Data breach response team leader	Only authorized persons can edit the files	Permanently
Contact details	Google drive of Data breach response team leader	Data breach response team leader	Only authorized persons can edit the files	Permanently
Documented decisions of the Data Breach Response Team	Google drive of Data breach response team leader	Data breach response team leader	Only Data Breach Response Team leader can edit the files	5 years
Data breach notifications	Google drive of Data breach response team leader	[Data breach response team leader	Only Data Breach Response Team leader can edit the files	5 years
Data Breach Register	Google drive of Data breach response team leader	Data Protection Officer	Only Data Protection Officer can edit the files	Permanently

12. Validity and document management

This document is valid as of March 2018.

The owner of this document is the Data Protection Officer who must check and, if necessary, update the document at least once a year.

Data Protection Officer
Simeon Drage

_____
[signature]