PERSONAL DATA BREACH NOTIFICATION PROCEDURE (TIER 2)

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) of Cognus are required to be aware of, and to follow this procedure in the event of a personal data breach (reference Training Policy GDPR DOC 1.1).

2.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Head of Resources.

3. Procedure – Breach notification data processor to data controller

3.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) of Cognus are required to report any data breach to the Head of Resources immediately. The Head of Resources will escalate to the Managing Director and Services Director without undue delay.

3.2 Cognus, through the Head of Resources, then reports any personal data breach or security incident to the data controller without undue delay. These contact details are recorded in the Internal Breach Register (GDPR REC 4.5). Cognus provides the controller with all of the details of the breach.

3.3 The breach notification at each stage is made by telephone and followed up with a confirmation email.

3.4 A confirmation of receipt of this information is made by email.

4. Procedure – Breach notification data controller to Information Commissioners Office

4.1 Cognus, through an emergency meeting of the Information Security Committee and in liaison with the Data Protection Officer determines if the Information Commissioners Office need to be notified in the event of a breach.

4.2 The Board of Directors is informed, via the Chair of the Board, if the outcome of the Information Security Committee meeting is that a breach has occurred and the Information Commissioners Office need to be notified.

4.3 Cognus assesses whether 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, by conducting a data protection impact assessment against the breach *GDPR REC 4.4*.

4.4 If a risk to data subject(s) is likely, Cognus reports the personal data breach to the Information Commissioners Office without undue delay, and not later than 72 hours.

4.5 If the data breach notification to the supervisory authority is not made within 72 hours, Cognus's Head of Resources submits it electronically with a justification for the delay.

4.6 If it is not possible to provide all of the necessary information at the same time Cognus will provide the information in phases without undue further delay.

4.7 The following information needs to be provided to the supervisory authority (GDPR REC 4.5):

- 4.7.1 A description of the nature of the breach.
- 4.7.2 The categories of personal data affected.
- 4.7.3 Approximate number of data subjects affected.
- 4.7.4 Approximate number of personal data records affected.
- 4.7.5 Name and contact details of the Head of Resources.
- 4.7.6 Consequences of the breach, both current and future.
- 4.7.7 Any measures taken to address the breach.
- 4.7.8 Any information relating to the data breach (this may be submitted in phases).

4.8 The Head of Resources notifies the Information Commissioners Office. Contact details for the Information Commissioners Office are recorded in the Schedule of authorities and key suppliers (GDPR-C REC 6.1.3).

4.9 In the event the Information Commissioners Office assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register GDPR REC 4.5.

4.10 The breach notification is made by email and copied to the Managing Director.

4.11 A confirmation of receipt of this information is made by including a read receipt on the email.

5. Procedure – Breach notification data controller to data subject

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Cognus via the Head of Resources, notifies those/the data subjects affected immediately by email or Special Delivery Royal Mail post.
5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4.6 above.
5.3 Cognus takes measures to render the personal data unusable to any person who is not authorised to access it using encryption.
5.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur by ensuring compliance with the GDPR.
5.5 If the breach affects a high volume of data subjects and personal data records, Cognus makes a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the Cognus's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner. GDPR DOC 7.4 should be used.
5.6 If Cognus has not notified the data subject(s), and the Information Commissioners Office considers the likelihood of a data breach will result in high risk, Cognus will communicate the data breach to the data subject by email or Special Delivery Royal Mail.
5.7 Cognus documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

Document Control

The Head of Resources is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of staff on the Intranet.

This procedure was approved by the Managing Director on 25/05/2018 and is issued on a version controlled basis under his/her signature.

Signature:  Date: 25/05/2018

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Managing Director	25/05/2018