Personal Data Breach Reporting Policy
Tinopolis Group:

1. About this document

1.1 This policy describes the actions that must be taken to report any incident which may result in a personal data breach. It applies whether or not a Group company is acting as a Data Controller or Data Processor in respect of the Personal Data.

1.2 It is the responsibility of all employees to read and adhere to the procedures detailed in this document. Any breach of this policy may result in disciplinary action.

2. Definitions

2.1 A **personal data breach** is defined in Article 4(12) of the General Data Protection Regulation as:

> "*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.*"

2.2 When an incident first comes to light, it may not be possible to determine whether or not it constitutes a personal data breach. The term **incident** is used in this policy to describe any situation which may, upon investigation, turn out to be a personal data breach. If an incident does not meet the definition of a personal data breach, it is described in this policy as a **near miss**.

2.3 This policy should be read in conjunction with our Data Protection Policy, which contains definitions of other terms used in this policy.

3. Identifying an incident

3.1 An incident may come to light in a number of ways. For example, it could occur by:

(a) direct observation by a member of staff – for instance, where an employee spots that personal data has been sent to the wrong email address;

(b) being reported to us by a third party, such as a supplier; or

(c) an audit / data protection review revealing that an incident has occurred.

4. Actions to take once an incident has been identified

4.1 Whenever an incident is identified, the following actions must be taken:

	Action	Responsibility	Timelines
1	Report the incident to Manager (Managing Director / Head of Production)	The employee who was first made aware of the incident	**Immediately the incident is identified**
2	Investigate and identify the full details of	Manager (with the assistance of the employee	**As soon as possible following the incident**

	the incident to identify the cause	who reported the incident)	**being identified**
3	Identify any immediate remedial action (see section 6, below)	Manager (with support from the Data Protection Manager (Sara Bond) and Group Finance Director (Jennifer Roberts))	**As soon as possible following the incident being identified**
4	Complete a Personal Data Incident Reporting Form (see **Appendix 1**) and return it to the Data Protection Manager	Manager	**Within 48 hours of the incident being identified**
5	Review the Personal Data Incident Reporting Form and decide whether the incident: 1) constitutes a personal data breach and, if so; 2) should be notified to the Customer, to the ICO and/or to data subjects	Data Protection Manager in consultation with Group Finance Director	**As soon as possible following step 4**
6	If necessary, notify the personal data breach to: 1) the Customer 2) the ICO 3) data subjects	Data Protection Manager in consultation with Group Finance Director	**Notification to the ICO must be without undue delay and in any event within 72 hours of the company becoming aware of the breach**
7	Check that all actions have been completed and close the incident	Data Protection Manager in consultation with Group Finance Director	**Once all actions have been completed**

5. Reporting a personal data breach

5.1 Our obligations to report a personal data breach depend on whether we are acting as a Controller or a Processor.

5.2 Where we are the **Controller**:

(a) We must report a personal data breach to the Information Commissioner's Office (**ICO**) 'without undue delay' and in any event within 72 hours of us becoming aware of the breach. We will be aware of the breach once we have decided that it meets the definition of a personal data breach. Depending on the circumstances, this could be immediately the incident is discovered or only after the incident has been investigated.

(b) There is an exception to this reporting requirement where the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected. A decision on whether the breach must be reported to the ICO will be made by the Data Protection Manager in consultation with the Group Finance Director and CEO and recorded on the Personal Data Incident Reporting Form.

(c) Where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals affected, there is an obligation to notify those individuals of the breach 'without undue delay'. The Data Protection Manager in consultation with the Group Finance Director and CEO will make the final decision as to whether notifying individuals is required and the decision recorded on the Personal Data Incident Reporting Form.

(d) As well as the requirement to report personal data breaches to the ICO, it may also be necessary to report certain incidents to the police. This should only be undertaken following consultation with the Data Protection Manager in consultation with the Group Finance Director and CEO.

5.3 Where we are the **Processor**:

(a) We must report the personal data breach to the Controller 'without undue delay'. We may also have specific contractual obligations to our customers to report personal data breaches to them within specified timescales.

6. Taking remedial action

6.1 As soon as the incident has been discovered and investigated, the appropriate manager should take remedial action to minimise the impact of the incident.

6.2 Remedial action should seek to mitigate any risks as a result of the breach, prevent similar breaches occurring in future, and/or protect our reputation. Action will depend on case specifics but may include may include the following:

(a) if personal data has been disclosed to a third party in error, it should be retrieved from the third party or deleted from the third party's IT system;

(b) if the incident arose as a result of an IT issue, the source of the issue should be identified and rectified; or

(c) if the breach arose as a result of human error, the individual should be made aware of the error and where appropriate asked to undertake additional training or be subjected to disciplinary action (this would usually only be appropriate in serious cases).

7. Follow-up action

7.1 To ensure that we learn from our mistakes, we will ensure that the causes of any personal data breach are analysed and, where appropriate, action is taken to ensure similar breaches do not occur again.

7.2 A copy of all Personal Data Incident Reporting Forms will be kept by the Data Protection Manager.

Version Control

Date of Issue	Document Version	Change Details	Document Author
5 February 2018	01	Policy drafted	Blake Morgan LLP
11 July 2018	02	Contact details updated	Sara Bond

Appendix 1 - Personal Data Incident Reporting Form

The relevant manager is responsible for completing parts 1, 2 and 3 of this form. Please complete it with as much detail as possible. If you do not have sufficient information to complete all of the form, please complete everything you can.

The Data Protection Manager must complete part 4 of this form.

Part 1: Summary	
Name and department of person reporting:	
Date of report:	*[Please state the date you are completing the form]*
Time and date incident first identified:	
Time and date incident actually occurred (if different):	
Circumstances of the incident:	*[Please give a summary of what actually happened]*
Part 2: Details of the personal data incident	
Nature of the incident:	[e.g. *which rules/procedures were breached and how did it happen? If you are not sure of the rules, just explain which internal procedure was not followed or ask the Data Protection Manager for assistance]*
Categories of data subject affected:	[*e.g. employees, members of the public, customers of our client]*
Approximate number of data subjects affected (if known):	
Possible consequences of the incident for data subjects:	*[State if there is likely to be any detriment to individuals. If yes please provide details]*

Part 3: Remedial actions	
What mitigating action was taken or will be taken in response to the incident?	
Follow up action taken to prevent similar future breaches:	
Part 4: Reporting the incident	
Does the incident constitute a personal data breach?	Y / N
If it is a personal data breach, is it notifiable to: • our customer (if we are a Processor)? • the ICO? • data subjects?	
Date(s) of notification:	
Date incident closed:	