Personal Data Breach Notification Policy

SCOPE

1. This personal data breach notification policy (the "Policy") applies to Tang & Co ("Tang & Co").
2. This Policy:
    a. forms part of Tang & Co's Data Protection Policy; and
    b. may be amended by Tang & Co at any time, consistent with the requirements of applicable laws and regulations. Any revisions will take effect from the date on which the amended Policy is published, as indicated in the version number set out herein.

DEFINITION

3. "Data Subject" is as defined in the Data Protection Policy.
4. "Internal Breach Register" means the internal breach register which details any Personal Data Breaches.
5. "Personal Data" is as defined in the Data Protection Policy.
6. "pseudonymised data" means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person and "pseudonymised" and "pseudonymisation" shall be construed accordingly.
7. "Sensitive Personal Data" is as defined in the Data Protection Policy.
8. "Supervisory Authority" means the Information Commissioner's Office (ICO), the UK's data protection supervisory authority.
9. Words denoting the singular shall include the plural and vice versa.
10. Unless otherwise stated, all defined terms have the same meaning as defined in the Data Protection Policy.

WHAT IS A PERSONAL DATA BREACH?

11. A "Personal Data Breach" is 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.
12. Examples of Personal Data Breaches are:

a. “Confidentiality breach” – an unauthorised or accidental disclosure of or access to Personal Data;

b. “Availability breach” – an unauthorised or accidental loss of access to or destruction of Personal Data;

c. “Integrity breach” – an unauthorised or accidental alteration of Personal Data.

PROCEDURE – ASSESSING A PERSONAL DATA BREACH

13. Tang & Co may be required to report Personal Data Breaches to the supervisory body no later than 72 hours after becoming aware of it.

14. Each Personal Data Breach must have a risk assessment performed to determine the extent and risk to the Personal Data. The risk assessment is based on facts and determines whether the Personal Data was used or disclosed in a way not permitted under Tang & Co’s policies. The risk assessment includes an evaluation of whether the incident compromises an individual’s Personal Data.

15. For the risk assessment the following steps will be carried out:

    a. Data list: A list and description of the data involved in the Personal Data Breach needs to be prepared. The list must include all the Personal Data which is potentially at risk as a result of the incident.

    b. Security controls applied to the data: Any security controls applied to the data may limit unauthorised exposure. The security controls applied to the data should be documented.

    c. Determination of risk to the individual: The level of risk to the individual will determine whether the Personal Data Breach is to be notified to the Supervisory Authority and/or the affected Data Subject. Determining the risk requires an evaluation of:

        c.i. the facts surrounding the Personal Data Breach;

        c.ii. an examination of the type of Personal Data;

        c.iii. the potential harm to the individual; and

        c.iv. security controls applied.

16. The following factors (along with any other relevant considerations) will be considered to determine if Personal Data has been compromised:

    a. the nature of the Personal Data Breach including where possible, the categories and approximate number of individuals concerned, and the categories and approximate number of data records concerned;

    b. the nature and extent of the Personal Data involved;

c. the identity of the unauthorised person who triggered the Personal Data Breach and, where applicable, or to whom it was disclosed;

d. whether the Personal Data was actually acquired (including whether any security controls were applied to prevent access);

e. the likely consequences of the Personal Data Breach; and

f. the measures that could be taken to address the Personal Data Breach.

PROCEDURE – BREACH NOTIFICATION TO SUPERVISORY AUTHORITY

17. If it is determined that a Personal Data Breach has occurred, Tang & Co will assess 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. Such a risk if unaddressed is likely to have a significant detrimental effect on individuals – for example, resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

18. If a risk to Data Subject(s) is likely, Tang & Co must report the Personal Data Breach to the Supervisory Authority without undue delay, and not later than 72 hours of becoming aware of the breach.

19. If it is not possible to provide all of the necessary information at the same time, Tang & Co will provide the information in phases without undue further delay. For the avoidance of doubt, even if all of the necessary information is not available, the Supervisory Authority must be contacted within the 72 hour deadline, and be provided with the information that is available and reasons why the remaining information is not available and expected timeframes when it will be provided.

20. The following information needs to be provided to the Supervisory Authority:

    a. a description of the nature of the Personal Data Breach;

    b. the date the Personal Data Breach occurred;

    c. the date the Personal Data Breach was discovered and any reasons why the breach was not notified within 72 hours (if applicable);

    d. the categories of Data Subjects affected;

    e. whether the Personal Data Breach involved pseudonymised data or anonymised data;

    f. approximate number of Data Subjects affected;

    g. the categories of Personal Data records affected;

    h. approximate number of Personal Data records affected;

    i. name and contact details of Tang & Co;

j. the likely consequences of the breach; and

k. any measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects.

21. Tang & Co will notify the Supervisory Authority.

22. In the event the Supervisory Authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

23. The breach notification is made to the Supervisory Authority by email with a follow up telephone call.

PROCEDURE – BREACH NOTIFICATION TO DATA SUBJECT

24. If the Personal Data Breach is likely to result in high risk to the rights and freedoms of the Data Subject, Tang & Co must notify the Data Subjects affected without undue delay.

25. The notification to the Data Subject should describe the breach in clear and plain language and contain at least the following information:

    a. name and contact details of Global DPO;

    b. likely consequences of the Personal Data Breach; and

    c. measures taken or proposed to be taken to address the Personal Data Breach, including where appropriate, to mitigate any adverse effects.

26. Such notification to the Data Subject referred to is not required if:

    a. Tang & Co 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. Tang & Co has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects referred are no longer likely to materialise; or

    c. it would involve disproportionate effort – in such a case, there shall instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

INTERNAL REGISTER

27. Tang & Co must keep an Internal Breach Register documenting any Personal Data Breaches which include:

    a. the facts relating to the Personal Data Breach;

    b. the effects of the Personal Data Breach; and

c. the remedial action taken.

DOCUMENT CONTROL

28. This Policy was approved as stated in this Section and is issued on a version-controlled basis.

Version	Date of Issue	Approved by	Position
1	21/05/18	Garry Tang	Principal