Tacconis Advisors & Co. LLP Data Breach Policy

1. Overview

Data breaches are increasingly common occurrences whether caused through human error or malicious intent. Tacconis Advisors & Co. LLP ("TAC") operations rely on the proper use of Confidential Information and Personally Identifiable Information on a daily basis. Managing risk and responding in an organised way to Incidents and Breaches is key to our operations.

2. Purpose

TAC must have a robust and systematic process for responding to reported data security Incidents and Breaches. This policy is designed to standardise the wide response to any reported Breach or Incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines. Standardized processes and procedures help to ensure that TAC can act responsibly, respond effectively, and protect its information assets to the extent possible.

3. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

4. Policy

A. General Information

A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and / or personal data. Data breaches are generally recognised as one of the more costly security failures of organisations. They could lead to financial losses, and cause consumers to lose trust in TAC or our clients.

Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

- Hacking attack
- 'Blagging' offences where information is obtained by deceit for the purposes of this policy data security breaches include both confirmed and suspected incidents.

B. Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary;
- Maintain a register of compliance failures;
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

Who to Notify:

- Notify Data Protection Officer ("DPO") if a data breach involves sensitive personal data;
- Notify individuals whose personal data have been compromised;
- Notify other third parties such as banks, credit card companies or the police, where relevant;
- The relevant authorities (e.g. police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (e.g. hacking, theft or unauthorised system access by an employee).

When to Notify:

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data;
- Notify affected individuals when the data breach is resolved.

How to Notify:

- Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, mobile messaging, SMS, e-mails, telephone calls);
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:

How and when the data breach occurred, and the types of personal data involved in the data breach.

- What TAC have done or will be doing in response to the risks brought about by the data breach;
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

C. Responding to a Data Breach

Upon being notified of a (suspected or confirmed) data breach, the DPO should immediately activate the Data Breach & Response Plan.

DPO response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

D. Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.