TIGERS

DELIVERING PEACE OF MIND

DATA BREACH POLICY AND PROCEDURE

CONTENTS

TABLE OF CONTENTS 1

PURPOSE 2

SCOPE 3

POLICY 4

TIGERS EUROPE – IMPORTANT INFORMATION 5

1. Purpose

Tigers holds and processes personal data on behalf of its staff and clients, of which the group has a responsibility to ensure that data breaches and /or information governance incidents are reported and managed efferently and effectively. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a security breach that could compromise data. Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, detrimental effect on our service provision, legislative noncompliance, and/or financial costs including significant fines from the local authorities.

The company is obliged under the Data Protection Act to have in place systems designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.
Under the Data Protection Act notification is mandatory for all controllers of private information, unless a breach is unlikely to result in a risk to the right of an individual. Tigers can get fined for data breaches and/or not complying to report a breach. The size of the fine is relevant to the risk. It is important in the event of a breach to act, investigate, manage and report the data breach as quickly as possible.

All Tigers employees that process information should notify any breaches to their Manager. Managers in turn will escalate this breach with processes in place to contain a breach, notify the relevant authorities if necessary and communicate to the individuals concerned when necessary.

What is the difference between an incident and a breach?

An incident is where there is a risk of a breach, by reporting these quickly, steps can be taken to investigate and secure the information to prevent a breach.

An information security breach is where the incident has resulted in any loss, or unauthorised access to data, normally involving personal or confidential information.

2. Scope

This Policy relates to all personal and sensitive data controlled or processed by the company regardless of format. This Policy applies to all employees, contractors, consultants, temporary staff, and other workers at Tigers and data processors working for, or on behalf of the company.

2.1. Types of Personal Data Breaches

2.1.1. Confidentiality breach

Where there is an unauthorised or accidental disclosure of, or access to, personal data. For Example:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it.
- Our customer database being compromised, for example being accessed by another customer.
- paper records containing personal data being left unprotected for anyone to see, for example: files left out when the staff member is away from their desk and at the end of the day,
- Papers containing personal information not properly disposed of in confidential shredding bins, papers left at printers.
- staff accessing or disclosing personal data outside the requirements or authorisation of their job.
- being deceived by a third party into improperly releasing the personal data of another person.

2.1.2. Availability breach

Where there is an accidental or unauthorised loss of access to, or destruction of, personal data. For Example:

- loss or theft of laptops, mobile devices, or paper records containing personal data.
- the loss of personal data due to unforeseen circumstances such as a fire etc.
- when there has been a permanent loss of, or destruction of, personal data.

2.1.3. Integrity breach

Where there is an unauthorised or accidental alteration of personal data. For Example:

- The removal and/or false alteration of individuals' mobile numbers, email addresses on home addresses

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, availability, and integrity of personal data at the same time, as well as any combination of these.

3. Policy

On discovery of a data breach the following actions should be taken:-

1. Containment and recovery
2. Assessing the risk
3. Notification of breach to the relevant authority
4. Evaluation and response.

3.1 Containment and Recovery

The staff member that might have committing the breach or having identified a possible breach should immediately inform their line manager or the Information Security Officer.

The priority is to contain the breach and limit its impact.

- Where personal data has been seen, accessed, or been sent to someone who does not have a legitimate need to see it, Tigers staff members should contact the recipient and:
  - tell the recipient not to pass it on or discuss it with anyone else.
  - tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so.
  - warn the recipient that it is illegal to use and or disclose data that was not intended for them.
- Where data has been lost, compromised and/or has become unavailable, then access to the data should be resumed as quickly as possible via backup copies of the data if necessary.
- In the event that the data controller is an outsourced client of Tigers, the person responsible for Data protection or breach notification should be given an initial notification advising what recovery processes are being performed with further information about the breach provided This is important to advise asap to meet the requirements by the local authorities of notification of breach within 72 hours (depending on the scope and size of breach)

3.2 2. Assessing the risk

A Breach Notification incident should be logged centrally with Internal IT support system, stating date and time of breach, how was breach detected, who committed breach, full details of breach, data subjects involved, action already taken, further action if necessary, on the Internal IT Support system.

The Information Security Officer and/or Data Protection Officer or a nominated person will conduct an investigation into the breach and prepare a Report.

This report will follow the local authority guidelines (for example Information Commissioner's Office) on Breach Management and will consider the following:

1. How the breach occurred.
2. The type of personal data involved.
3. The number of data subjects affected by the breach.
4. Who the data subjects are.
5. The sensitivity of the data breached.
6. What harm to the data subjects can arise? For example, the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.
7. What could happen if the personal data is used inappropriately or illegally?
8. For personal data that has been lost or stolen, are there any protections in place such as encryption? 9. The measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
9. Whether the breach should be notified to the ICO – if NOT the reasoning behind this decision including reasons why the breach is unlikely to result in a risk to the rights and freedoms of individuals.

3.3. Breach notification

In the likelihood that an adverse effect has occurred, and the adverse effect is low, the incident is not reportable to the local authorities; for example ICO; and no further details will be required.

However, should there be an adverse effect on individuals for example potential pain and suffering of individuals/potential financial losses sustained the local authorities should be notified within 72 hours of the breach.

3.3.1. To the Local authorities

Under Article 33 of the GDPR – In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Data Protection Officer or information Security Officer or in the absence of either of these people, any member of the Senior Leadership Team, will determine whether the breach is one which is required to be notified to the local authority.

NOTE: Each country will have their own local authorities. The data protection officer or information security officer of the country should contact their local authority.

3.3.2. To the affected individuals

If a breach is also assessed to be likely to result in a high risk to the rights and freedoms of individuals (this could be staff, customers etc) , the individuals themselves must be informed directly and without undue delay, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

When informing the individuals, the following needs to be supplied in clear and plain language:

1. the nature of the personal data breach,
2. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
3. a description of the likely consequences of the personal data breach; and
4. a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

3.4. Evaluation and response

Once the breach has been dealt, evaluation need to take place with need to feed back into staff training, awareness sessions to mitigate incidents occurring in the future.

4. Tigers Europe – Important Information

United Kingdom:

Tigers Global Logistics Ltd (GB)
812 Oxford Avenue, Slough, Berkshire, SL1 4LN, UK

Data Protection Officer:
Tania Zaaiman
Tel: +44 1784 266400
Mob: +44 (0) 7917274600
tania.zaaiman@go2tigers.com

Data Protection Authority
Information Commissioners Office
TeL: +44 0303 123 1113
https://ico.org.uk/for-organisations/report-a-breach/

The Netherlands:

Tigers International Logistics BV (NL)
Schaapherderweg 24, 2988 CK Ridderkerk, The Netherlands

Data Protection Officer:
Joost de Puy – Data Protection Officer
Tel: +31 180 20 9808
Mob: +31 6 11 389 347
joost.depuy@go2tigers.com

Data Protection Authority
Autoriteit Persoonsgegevens
Tel: +31 (0)70 – 888 85 00
https://autoriteitpersoonsgegevens.nl/en/news/data-breach-notification-obligation

Germany:

Tigers GmbH (DE)
Munich Airport Business Park, Ludwigstraße 44, 85399 Hallbergmoos, Germany

Data Protection Officer:
Maximilian Ernst – Data Protection Officer
Tel: +49 811 880 186
Maximilian.Ernst@Go2Tigers.com

Bavarian Authority
Bayerisches Landesamt für Datenschutzaufsicht
https://www.lda.bayern.de/de/index.html

Federal Authority
Die Datenschutzaufsichtsbehörden
Tel: +49 (0) 681 94781-0
https://www.datenschutzkonferenz-online.de/datenschutzaufsichtsbehoerden.html

TIGERS (HK) CO LTD
4B Kenning Industrial Building, 19 Wang Hoi Road, Kowloon Bay, Hong Kong, China
T: +852 2215 5500 F: +852 2754 1000
www.go2tigers.com