GDPR DATA BREACH POLICY AND RESPONSE PLAN

Introduction

Under the General Data Protection Regulation (GDPR), certain personal data breaches must be notified to the Information Commissioner's Office (ICO) and sometimes affected data subjects need to be told too.

The purpose of this policy is to outline the Company's internal breach reporting procedure and the Company's internal and external response plan and it should be read in conjunction with the Company's data protection policy.

What constitutes a personal data breach?

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"*.

A breach is therefore a type of security incident and there are three different types of breaches that may occur:

1. Confidentiality breach - an accidental or unauthorised disclosure of, or access to, personal data.
2. Availability breach - an accidental or unauthorised loss of access to, or destruction of, personal data.
3. Integrity breach - an accidental or unauthorised alteration of personal data.

A breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

A personal data breach would, for example, include:

- loss of personal data, e.g. loss or theft of a Company smartphone or laptop which holds personal data such as a customer or client database, or where the only copy of personal data has been encrypted by ransomware and the data cannot be restored from backup
- personal data being disclosed to an unauthorised person, e.g. an employee's payslip being sent to the wrong person
- an unauthorised person accessing personal data, e.g. an employee's personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls
- a temporary or permanent loss of access to personal data, e.g. where a client's or customer's personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or

TipsTrade Ltd. Unit16, Wornal Park, Menmarsh Road, Worminghall, AYLESBURY, HP18 9JX
TipsTrade Ltd. Registered in England No. 4676520 VAT No: 816 0175 52
Registered Office: 6a St. Andrews Court, Wellington Street, THAME, OX9 3WT

by an unauthorised person or where the decryption key for securely encrypted data has been lost.

This list is not exhaustive.

Notification to the ICO

Not all personal data breaches have to be notified to the ICO. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Company on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If the Company's report is submitted late, it must also set out the reasons for the delay. Notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- the name and contact details of the Company's data compliance manager
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

The Company can provide this information in phases, without undue further delay, if it cannot all be provided at the same time.

Awareness of the breach occurs when the Company has a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach.

However, where it is unclear whether or not a breach has occurred, the Company will have a short period of time to carry out an initial investigation after first being informed about a potential breach in order to establish with a reasonable degree of certainty whether or not a breach has in fact

occurred.

If, after this short initial investigation, it is established that there is a reasonable degree of likelihood that a breach has occurred, the 72 hours starts to run from the moment of that discovery.

Communication to affected data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Company also needs to communicate the breach to the affected data subjects without undue delay, i.e. as soon as possible. In clear and plain language, the Company must provide them with:

- a description of the nature of the breach
- the name and contact details of the Company's data compliance manager
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

The Company will also endeavour to provide data subjects with practical advice on how they can themselves limit the damage, e.g. cancelling their credit cards or resetting their passwords.

The Company will contact data subjects individually, which may be by letter, e-mail or text message, unless that would involve the Company in disproportionate effort, such as where their contact details have been lost as a result of the breach or were not known in the first place, in which case the Company will use a public communication, such as a notification on the Company's website, issuing a public statement or a prominent advertisement in print media.

However, the Company does not need to report the breach to data subjects if:

- the Company has implemented appropriate technical and organisational protection measures, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

Assessing "risk" and "high risk"

In assessing whether a personal data breach results in a risk or high risk to the rights and freedoms of data subjects, the Company will take into account the following criteria:

- the type of breach
- the nature, sensitivity and volume of personal data affected
- ease of identification of data subjects - properly encrypted data is unlikely to result in a risk if the decryption key was not compromised in the breach
- the severity of the consequences for data subjects
- any special characteristics of the data subject
- the number of affected data subjects
- special characteristics of the Company.

Data breach register

The Company will maintain a register of all personal data breaches, regardless of whether or not they are notifiable to the ICO. The register will include a record of:

- the facts relating to the breach, including the cause of the breach, what happened and what personal data were affected
- the effects of the breach
- the remedial action the Company has taken.

Data breach reporting procedure

If you know or suspect that a personal data breach has occurred, you must immediately both advise your line manager and contact the Company's data compliance manager. They can be contacted as follows: . You must ensure you retain any evidence you have in relation to the breach and you must provide a written statement setting out any relevant information relating to the actual or suspected personal data breach, including:

- your name, department and contact details
- the date of the actual or suspected breach
- the date of your discovery of the actual or suspected breach
- the date of your statement
- a summary of the facts relating to the actual or suspected breach, including the types and amount of personal data involved
- what you believe to be the cause of the actual or suspected breach
- whether the actual or suspected breach is ongoing
- who you believe may be affected by the actual or suspected breach.

You must then follow the further advice of the data compliance manager. You must never attempt to investigate the actual or suspected breach

yourself and you must not attempt to notify affected data subjects. The Company will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and the data breach team will determine who should be notified and how.

Response plan

The Company's data compliance manager will assemble a team to investigate, manage and respond to the personal data breach. They will lead this team and the other members will consist of nominated senior members of the management team. The data breach team will then:

1. Make an urgent preliminary assessment of what data has been lost, why and how.
2. Take immediate steps to contain the breach and recover any lost data.
3. Undertake a full and detailed assessment of the breach.
4. Record the breach in the Company's data breach register.
5. Notify the ICO where the breach is likely to result in a risk to the rights and freedoms of data subjects.
6. Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.
7. Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist the data breach team in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of data subjects.

Example	**Notify the ICO?**	**Notify data subjects?**	**Notes**
The Company stored a backup of an archive of personal data encrypted on a CD and the CD is stolen during a burglary	No	No	As long as the personal data are encrypted with a state-of-the-art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data are exfiltrated from a secure website managed by the Company during a cyber-attack	Yes, if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to data subjects is high	If the risk is not high, the Company can still notify data subjects, depending on the circumstances of the case
A brief power outage lasting several minutes means that clients are unable to call the Company and access their records	No	No	This is not a notifiable personal data breach, but it is still a recordable incident
The Company suffers a ransomware attack which results in all personal data being	Yes, if there are potential consequences to	Yes, depending on the nature of the	If there was a backup available and personal data could be restored in good time, this would

TipsTrade Ltd. Unit16, Wornal Park, Menmarsh Road, Worminghall, AYLESBURY, HP18 9JX
TipsTrade Ltd. Registered in England No. 4676520 VAT No: 816 0175 52
Registered Office: 6a St. Andrews Court, Wellington Street, THAME, OX9 3WT

encrypted, no backups are available and the personal data cannot be restored On investigation, it becomes clear that the ransomware's only functionality was to encrypt the personal data, and that there was no other malware present in the system	individuals as this is a loss of availability	personal data affected and the possible effect of the lack of availability of the personal data, as well as other likely consequences	not need to be reported to the ICO or to data subjects as there would have been no permanent loss of availability or confidentiality
An employee reports that they have received a monthly payslip for another employee and a short investigation reveals that it is a systemic flaw and other employees may be affected	Yes	Only if there is high risk	If, after further investigation, it is identified that more employees are affected, an update to the ICO must be made and the Company must take the additional step of notifying those other data subjects if there is high risk to them
The Company's website suffers a cyber-attack and customers' login usernames, passwords and purchase history are published online by the attacker	Yes	Yes, as could lead to high risk	The Company should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk
Clients' personal data are mistakenly sent to the wrong mailing list	Yes	Yes, depending on the scope and type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients	Yes, notifying	Yes, depending	Notification may not be necessary if no sensitive

TipsTrade Ltd. Unit16, Wornal Park, Menmarsh Road, Worminghall, AYLESBURY, HP18 9JX
TipsTrade Ltd. Registered in England No. 4676520 VAT No: 816 0175 52
Registered Office: 6a St. Andrews Court, Wellington Street, THAME, OX9 3WT

in the "to:" or "cc:" fields, thereby enabling each recipient to see the e-mail address of other recipients	may be obligatory if a large number of individuals are affected, if sensitive personal data are revealed or if other factors present high risks, e.g. the e-mail contains passwords	on the scope and type of personal data involved and the severity of possible consequences	personal data is revealed and if only a minor number of e-mail addresses are revealed