# Tommy's Personal Data Breach Policy

## 1. Introduction

A **personal data breach** is a security incident which affects the confidentiality, integrity or availability of personal data. A **near miss** is a security incident which is prevented from becoming a personal data breach, often through early intervention such as containment.

This policy describes how Tommy's manages personal data breaches and near misses. All employees and users of Tommy's personal data are responsible for observing this policy and procedure.

## 2. What is a personal data breach?

A personal data breach leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. The breach may be deliberate or accidental, and occurs through the action or inaction of a controller or processor.

Examples include:

- Permitting access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Losing a mobile computing device which contains personal data
- Altering personal data without permission
- A computer system being compromised (eg by a virus or malware)
- A break-in at an office which holds critical information-processing equipment such as servers.

## 3. What risks may a personal data breach incur?

If not addressed in an appropriate and timely manner, a data breach can result in a loss of control over individuals' data, a limitation of individuals' rights, discrimination, identify theft or fraud, financial loss, damage to reputation or a loss of confidentiality.

Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. But other breaches can significant affect individuals, causing emotional distress and physical and material damage.

## 4. What does Tommy's do if there is an apparent data breach or near miss?

Tommy's investigates and records all apparent data breaches and near misses, whether or not they need to be reported to the ICO or individuals, using the Investigation Record of Data Breach and Near Misses form at Appendix 1. Our record includes:

- The facts relating to the breach
- The effect of the breach
- Whether the breach is reportable to the ICO
- Whether the breach is reportable to individuals
- The remedial action taken
- Whether or not the breach was a result of human error or a systemic issue, and
- How a recurrence can be prevented (for example, through better processes, further training or other corrective steps).

## 5. When must a personal data breach be reported to the ICO?

When a personal data breach has occurred Tommy's seeks to contain it, and investigates to establish the likelihood and severity of the resulting risk (whether temporary or permanent) to people's rights and freedoms.

- If is **likely** that there will be a risk to rights and freedoms, then the Information Commissioner's Office (ICO) will be notified.

- If it is **unlikely** that there will be a risk to rights and freedoms, then the breach does not have to be reported. In this circumstance Tommy's documents the reason for its decision not to report the breach.

Near misses are not normally reported to the ICO. However, the ICO may be contacted for advice in such a situation.

## 6. What is the timescale for reporting a breach to the ICO?

Tommy's reports notifiable breaches to the ICO without undue delay and not later than 72 hours after becoming aware of it. If there is a delay Tommy's gives its reasons for the delay and explains when it expects to submit more information.

## 7. What information does Tommy's give to the ICO?

When reporting a breach Tommy's gives:

- A description of 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 personal data records

- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the personal data breach, and
- A description of the measures being taken or proposed to deal with the breach, including where appropriate mitigating any possible adverse effects.

Tommy's expedites the investigation, allocating sufficient resources to manage it urgently.

The General Data Protection Regulation (GDPR) recognises that it is not always possible to investigate a breach fully within 72 hours. Where this is the case Tommy's provides the required information in phases, without undue delay.

## 8. How does Tommy's notify a breach to the ICO?

We notify any reportable breach to the ICO either using the Helpline **0303 123 1113** or using the Personal Data Breach Reporting Form available at https://ico.org.uk/for-organisations/report-a-breach/

## 9. When does Tommy's notify individuals about a breach?

In accordance with the GDPR, if a breach is likely to result in a **high risk** to the rights and freedoms of individuals, the data controller (Tommy's) must inform those concerned directly and as soon as possible.

A **high risk** means that the threshold for informing individuals is higher than for notifying the ICO. To identify the level of risk presented by the breach, Tommy's conducts an assessment of:

- The severity of the potential or actual impact on individuals, and
- The likelihood of this occurring.

Where the impact of the breach is more **severe**, the risk is higher. Where the **likelihood** of the negative consequences is greater, then again the risk is higher.

Where a high risk is identified Tommy's notifies those affected promptly, particularly if there is a need to mitigate an immediate risk of damage to them.

If Tommy's decides not to notify individuals it documents the reason for taking this decision, and the Charity still notifies the ICO of any reportable breach.

Regardless of the outcome of Tommy's risk assessment, if the ICO identifies a high risk it may compel Tommy's to notify individuals. Therefore, when there is a reportable breach Tommy's takes advice from the ICO on whether data subjects need to be told.

## 10. What information does Tommy's provide to any individuals it notifies of a personal data breach?

Tommy's describes the nature of the personal breach in clear and plain language, giving at least the following information:

- The name and contact details of the Data Protection Officer
- A description of the likely consequences of the breach, and
- A description of the measures Tommy's is taking, or proposes to take, to deal with the breach, including where appropriate mitigating any possible adverse effects.

# TOMMY'S INVESTIGATION RECORD OF DATA BREACHES AND NEAR MISSES

| Topic | Investigation report |
|---|---|
| **Incident date** | |
| **Incident number** | |
| **Investigating officer (normally the Data Protection Officer)** | |
| **Report date** | |
| **Description of incident and likely consequences** | |
| **Has the information been recovered (if so, how)?** | |
| **Has the information been contained (if so, how)?** | |
| **Is this a breach or a near miss?** | |
| **If there has been a breach, is it likely that there is a risk to individual rights and freedoms?** | |
| **Has the ICO been notified? (If not, a reason for this decision should be inserted here.)** | |
| **If there has been a breach, is there a high risk to individual rights and freedoms?** | |
| **Have the individuals whose data has been breached been notified? (If not, a reason for this decision should be inserted here.)** | |
| **Root causes identified** | |
| **Lessons learned** | |

| | |
|---|---|
| **Recommendations** | |
| **Arrangements for shared learning** | |

**Signed_____**

**Data Protection Officer**

**Date_____**