February 2019

Notification of data breaches

General information about the notification

What is a data breach?

A data breach is a security breach that leads to the accidental or unlawful **destruction**, **loss**, **alteration**, unauthorised **disclosure** of, or unauthorised **access** to, **personal** data transmitted, stored or otherwise processed. Personal data is information that relates to a natural person or can be attributed to a natural person.

Examples of data breaches are:

- Loss of data as a result of the loss or theft of a laptop or of a mobile data storage device (USB flash drive, tablet, mobile phone, etc.);
- Transfer of personal data to an unauthorised recipient;
- Malware or hacker attacks on databases containing personal data;
- Accidental publication of personal data on the Internet;
- Emails sent to a public cc list that contains a large number of email addresses.

What data breaches need to be notified?

As a rule, each data breach must be notified to the competent data protection supervisory authority, unless the breach is unlikely to lead to a **risk to the rights and freedoms of natural persons**. A breach may lead to physical, material or non-material damage for natural persons, such as the loss of control over one's personal data or a restriction of rights, discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of protected personal data, or economic or social disadvantages for the data subjects concerned. If Tag GmbH as a so-called processor processes personal data on behalf of a customer and a data breach takes place in relation to personal data of this customer, Tag GmbH must enable the customer without delay to comply with its notification obligations.

This is why you are obliged to notify any incident without delay to your superior. Whether the incident requires notifying a data protection supervisory authority or the data subjects concerned will be examined and decided by the **Management** in consultation with the **Data Protection Officer** of Tag GmbH on a case-by-case basis, taking your statements into account.

Your Data Protection Officer

Dr. Stefanie Hellmich

Lawyer with Luther Rechtsanwaltsgesellschaft mbH

Phone +49 69 27229 24118

Notification of data breaches

What are the legal consequences if Tag GmbH fails to properly perform this notification obligation?

In the event of failure to notify a data breach that is required to be notified within the applicable period of time or of another violation of the notification obligations, the data protection supervisory authority may impose an administrative fine of up to EUR 10 million or equal to up to 2 percent of the worldwide sales of the Tag Group. Furthermore, the data subjects concerned may claim compensation for any material or non-material damage suffered.

What internal processes and instructions at Tag GmbH need to be observed?

In order to enable us to perform our notification obligations in due time and reduce the related risks, please observe the following instructions as to how to proceed:

Initial notification

As soon as you become aware of or suspect a data breach, please inform your superior as quickly as possible, either by phone or by email (**initial notification**).

Such an initial notification should be given in each particular case, even if you only have a suspicion or if you believe there is not much of a risk. This applies to both data breaches discovered by yourself and data breaches that are brought to your attention by a service provider or a third person (another member of staff or an external person). The Management will examine the circumstances in consultation with the Data Protection Officer and decide whether to take further action.

"Data breach" notification form

After you have given initial notification, please complete the attached "Data breach" notification form and send it to Sara Moir (sara@tagcs.com), who will examine the information provided in consultation with the Data Protection Officer and cause the appropriate notifications to be given, if necessary. Please treat the incident as confidential and do not disclose any information about the data breach to other staff – with the exception of your superior, the Head of IT, Tag GmbH Manager, the members of the Management, and the Data Protection Officer – or external third parties.

Your Data Protection Officer

Dr. Stefanie Hellmich

Lawyer with Luther Rechtsanwaltsgesellschaft mbH

Phone +49 69 27229 24118

stefanie.hellmich@luther-lawfirm.com

“Data breach” notification form

Please provide your name and your official contact details.

When did the data breach take place?

On or between *: _____ and _____

*If you do not know, please insert the approximate date or period.

When was the data breach discovered for the first time?

On: _____

Did you inform the Management / your superior of the detected or suspected data breach (initial notification)?

Initial notification on: _____ to*: _____

*Please give the name of your superior / of the person who was informed.

Reasons for the delay (if applicable): _____

Please specify the type of the detected or suspected data breach (e.g. theft, loss, or hacker attack).

Please describe the details and circumstances of the data breach (e.g. the procedures concerned, the parties or persons involved, the location where the breach took place, the devices/data storage media concerned, the security measures that were circumvented, etc.).

Please describe the categories and the approximate number of data subjects concerned (e.g. staff, customers, or children).

Please describe the categories of data concerned and the approximate number of files concerned. Does the data concerned include sensitive data (e.g. credit card data, health data, or identification data)?

Is the data concerned customer data that is being processed by Tag GmbH on behalf of customers?

What are the foreseeable consequences of the data breach?

What measures have been taken or are intended to be taken to deal with the data breach, including measures to keep the adverse consequences to a minimum?

Are other parties / companies involved (e.g. joint controllers, Group companies, service providers)?

Please provide any other relevant information and/or documentation that might be helpful in examining the incident.

Date, signature