Procedure for reporting and handling data breaches // Mopinion

Introduction

This document outlines the different steps taken by Mopinion in the event of a data breach, which falls under the data breach notification obligation (Meldplicht Datalekken). The data breach notification obligation is a modification to the Personal Data Protection Act (Wet Bescherming Persoonsgegevens), which entered into force with effect from January 1st, 2016. When there is a data breach, there is a security breach of personal data (referred to in Article 13 of the Personal Data Protection Act). The personal data is then exposed to loss or unlawful processing.

Data breaches can occur through:

- willfull action (cyber crime, hacking, identity theft, malware infection);
- technical failure (ICT malfunctions);
- human error (passwords are too simple/providing a username or password to colleagues and external contacts);
- disaster (fire in data centre, flooding);
- loss of USB stick or laptop;
- sending an e-mail including e-mail addresses of all recipients;
- as well as the unlawful processing of data (DDS application Shipping and Receiving Station for Customers/Buyers.

A data breach should be reported to the Authority for Personal Data immediately (within two days) after the person responsible (1) within Mopinion has been informed. The parties concerned must also be notified about the data breach. For Mopinion, these are generally customers (citizens and companies) or employees. Those involved are those whose personal data has been involved in an infringement. The person concernned must be informed immediately of the breach if the breach is likely to adversely affect his/her privacy. A processer (2) is required to report the data breach to the person responsible.

1. Person responsible: CTO (Chief Technology Officer) of Mopinion. The person responsible has control over the purpose and method of processing. Formally, legally and factually (functionally), he/she is the person who determines the purpose and method of processing personal data. The person who has this control and responsibility over purpose and method of processing also makes decisions about the retention periods, providing access requests, etc. The person responsible has the directive role (control of the privacy management in the chain);

2. Processor: the individual that processes the data on behalf of the person responsible without being subject to his/her direct authority (also externally). The processor processes personal data in accordance with the instructions and ultimate responsibility of th person responsible. The processor does not make decisions about the use of the data, the disclosure to third parties and other recipients, the duration of data storage, etc.

Report

All data breaches of personal data must be reported internally and documented by the Data Protection Officer (DPO). The report can be made by every employee and every processor. The report can also be made by an external contact or by an employee of Mopinion. The report must be sent out directly and by telephone to the DPO and it must be in writing. Our DPO reports the data breach, if necessary, to the Personal Data Authority.

The DPO establishes:
- name of the reporter;
- date and time of the report;
- nature of the infringement (is there a substantial risk of loss or unlawful processing?);
- the personal data in the report;
- which amount and/or data records is it regarding;
- which (groups) persons are involved in the report;
- which measures have been or will be taken by the reporter;
- what are the implications for those involved, according to the reporter;
- the contact person for the report.

First analysis

The DPO assess whether the infringement "can be reasonably assumed to lead to a significant risk of loss or unlawful processing, which adversely affects the privacy of the parties related." If this is not the case, then the DPO will carry out the following actions:

1. inform the CTO (Chief Technology Officer) of Mopinion by phone;
2. inform the manager of specific department officer by phone;
3. during office hours: directly convene the Data Breach Response team, consisting of: The DPO, CTO, manager responsible for the department where the breach was found, and a member of the controlling team. The DPO is responsible for reporting.

Outside office hours and over the weekend, a report is made by the DPO. If the DPO cannot be reached, the report is made by the CTO. If possible, the necessary meetings will be postponed and re-scheduled during office hours. If this is not possible, the meeting will be conducted by telephone and electronically.

Data Breach Response Team

The Data Breach Response Team, in case of a high priority, is convened by the DPO. The meeting is chaired by the DPO. The response team discusses and defines:

- the information that has been recorded by the DPO when drawing up the report;
- the necessary follow-up actions with regard to the data breach (immediately seal the leak, limit access to information and simultaneously gather more information about the intruder);
- what will reported by the DPO to the Personal Data Authority (aside from the nature of the infringement, which personal information, number of persons/records involved);
- the potential consequences for those involved;
- the measures Mopinion takes or can take to reduce the damages for those involved;

• the measures that those involved can take to further reduce damages, including the manner with which they are notified;
• contact information for those involved;
• the method of handling the breach internally, including communication with the one who reported the breach, the relevant department(s) and manager(s);
• whether there is personal liability, or third party liability, such as on account of breach of contract (because a confidentiality obligation has been breached, or inadequate security was realised which is in violation of a contractual obligation) or tort;
• assess whether to make a declaration and determine whether there is criminal culpability.
This can come into play when there is, for example, involvement from Mopinion itself, a processor, or when insufficient measures have been taken to prevent disturbances. If desired, the meeting will be held with the legal counsel;
• what is communicated internally and at what time;
• what is communicated externally and at what time. It is determined whether the press should be informed;
• if other stakeholders need to be informed, in addition to the Personal Data Authority;
• if other individuals and/or companies need to be informed;
• how it is reported internally, including the actionee;
• if any damage is covered by the insurance policy.

Continuation

The DPO reports the results of the Data Breach Response Team meeting to the CTO of Mopinion. The CTO either approves the activities to be carried out, as stipulated by the Data Breach Response Team, or adjusts them. The activities stipulated by the CTO are then carried out.

Reporting to the Personal Data Authority

The DPO reports the data breach to the Personal Data Authority (Personal Data Authority online form) within 2 days and according to the preferred method. The following must be reported, in any case:
• nature of the infringement, including categories involved, number of persons involved, number of data records;
• description of the anticipated effects;
• undertaken and/or proposed measures;
• Information about the measures that should be taken by the person involved, to limit the adverse effects;
• contact information for those involved;

Delivery confirmation of Personal Data Authority

If a report has been made, Mopinion will receive a delivery confirmation. In the reports that give rise to further action by the Authority, the Authority will contact Mopinion to verify the origin of the message.

Absence of DPO

In the event of absence, the DPO's role will be filled by either the CTO or Head of Support.