Data Breach Response Plan – Bedrijf Y B.V.

Date: 1 April 2019
Version: 5

2. What is a data breach?

2.1. Introduction

Not all data breaches need to be reported to the authorities. A data breach that will have to be reported to the Autoriteit Persoonsgegevens is defined as follows:

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.

The General Data Protection Regulation (GDPR) – that will replace the Wbp as of May 25, 2018 – speaks of a 'personal data breach'. This is a security breach that results, by accident or in an unlawful way, in the loss, alteration, or unauthorized disclosure or access to personal data that has been transfered, stored or processed otherwise. A breach does not need to be notified, when it is unlikely that this reasonably involves a risk for the data subjects.

To assess whether there is a data breach, three questions must be answered in the following order:

1. Was there a security breach?
2. Did this breach involve any leakage or loss of personal data?
3. Can it reasonably be ruled out that personal data has been lost or processed in an unlawful way?

Every question is one step leading to the decision whether there has been a data breach. These steps are explained below.

2.2. Security breach

There is only a security breach, when there has been an actual incident. Merely the danger of such a breach is not an actual incident, and therefore not a security breach.

Examples of security breaches are:

- a lost USB stick;
- a stolen laptop;
- an email is sent, with all receivers CC'd instead of BCC'd;
- attack by a hacker;
- a malware infection;
- a disaster such as a fire in a data center.

3. When should you notify a data breach to the authority?

3.1. Introduction

From the moment a data breach as described in section 2 has occurred. Bedrijf Y B.V. should assess whether this breach should be notified to the Autoriteit Persoonsgegevens (AP), the Dutch data protection authority. A data breach must be notified if it is likely to result in a risk to the rights and freedoms of natural persons.

This criterion is explained below.

3.2. Quantitatively serious

A data breach can be a risk if it involves a large number of data (quantitatively serious). For example, a breach in one of the databases of Bedrijf Y B.V., resulting in the public disclosure of 1000 customers of Bedrijf Y B.V., will be regarded to be quantitatively serious and will therefore have to be notified to the authority.

3.3. Qualitatively serious

A data breach can also be considered to be serious if it does not involve the loss of a large volume of personal data, but rather because it involves sensitive personal data (qualitatively serious). These are a few examples of sensitive personal data:

- login details
- financial data
- copies of ID cards
- criminal records
- data concerning performance at work
- data concerning religion or believes
- data concerning health

You should always consider both the nature and size of the data breach in assessing whether the breach should be notified to the authority. In any case, it is certain that a leak of login data should be notified to the authority, considering the qualitatively serious nature of such data.

Example: due to a security breach in the database of Bedrijf Y B.V., unauthorized persons obtained access to customer data, including outstanding payments. Such a breach of sensitive data should be notified to the data proection authority.

---

4. What should be reported to the authority?

The Autoriteit Persoonsgegevens requires to submit specific information in case a data breach should be notified. The required information is specified below.

About Bedrijf Y B.V.

- Name of the organization
- (Visiting) address
- Postal code
- Town
- Registration number of the Chamber of Commerce
- Sector in which Bedrijf Y B.V. operates

About the reporter

- Name
- Function
- E-mailaddress
- Phone number and alternative phone number

About the data breach

1. What is the nature of the incident?
    - o A device (e.g. phone or laptop), data carrier (e.g. USB stick) or paper got lost or stolen
    - o A letter or parcel got lost or was received opened
    - o Hacking, malware (e.g. ransomware) and/or phishing
    - o Personal data was found in the old paper stack
    - o Personal data were left on a discarded device
    - o Personal data were published by accident
    - o Personal data were sent or delivered to the wrong receiver
    - o Other
2. Provide a summary of the event, in which a violation of the security of the personal data has occurred.
3. Did the breach occur in a process outsourced to another organization (the processor)?
    - o Yes, namely:
    - o No
4. Name of the organization to which the data processing is outsourced.
5. What is the number of people, whose personal data are involved in the breach? (Please fill in the numbers.)
    - o Minimal: (fill in)
    - o Maximal: (fill in)

1. When did Bedrijf Y B.V. notify the data subjects, or when is Bedrijf Y B.V. planning to do this?
    - Bedrijf Y B.V. notified the data subjects on [date]
    - Bedrijf Y B.V. shall notify the data subjects on [date]
2. What is the content of the report to the data subjects?
3. How many data subjects did Bedrijf Y B.V. inform or is Bedrijf Y B.V. planning to inform?
4. Which mean(s) of communication did Bedrijf Y B.V. use, or is Bedrijf Y B.V. going to use, to inform the data subjects?
5. Why did Bedrijf Y B.V. refrain from notifying the data breach to the data subjects?
6. Are the personal data encrypted, hashed or made unintelligible or inaccessible in any other way to unauthorized persons? (Choose one of the following options and add where necessary.)
    - Yes
    - No
    - Partially, namely: (fill in)
7. If the personal data are (partially) made unintelligible or inaccessible, in which way has this been achieved? If Bedrijf Y B.V. makes use of encryption, please elaborate on the method of encryption.
8. Does the breach involve persons from other EU countries? (Please choose one of the following options.)
    - Yes
    - No
    - Unknown yet
9. Has Bedrijf Y B.V. notified the data breach to authorities in other EU countries?
    - Yes, namely: (fill in)
    - No
10. Is the notification complete in the view of Bedrijf Y B.V.?
    - Yes, the required information is complete and no subsequent report is necessary
    - No, there will be a subsequent report with further details on the breach

After the notification to the authority, a confirmation thereof will be sent to the e-mail address of the specified contact. Bedrijf Y B.V. must print and store this confirmation. This confirmation contains a number under which the notification is registered with the AP, which is necessary to modify or withdraw the notification.

Even when the data breach does not need to be notified to the data subjects because the data are unintelligible or inaccessible to unauthorized persons, it is necessary to assess whether the data are still unintelligible or inaccessible from time to time in the future (see also section 7). For example, when notification is not required (because of the use of encryption), but the used encryption becomes compromised after half a year, the law still requires to inform the data subjects of the data breach. It is also possible to proactively inform the data subjects after the data breach anyway, to prevent that data subjects have to be informed a long time after the data breach has occurred.

Please note: encryption or hashing does not offer any protection against the destruction or removal of personal data. Such data breaches shall always need to be repported to the data subjects, if they are negatively affected by the breach.

5.4. Term

The data breach must be notified to the data subjects 'without delay', which means: as soon as possible, allowing for some time to collect the correct information in order to make a careful report. In other words: the notification to the data subject must be carried out carefully, but may not be unduly delayed. The law does not require a fixed term like it does for the notification to the authority.

The data controller is responsible for the notification to the data subjects, unless agreed otherwise.

6. What should be reported to the data subjects?

The notification to data subjects must be carried out decently ad carefully, and at least contain the following information:

- Nature of the breach, where it is sufficient to provide a general description of the event;
- Where data subjects can go for questions, such as a phone number of customer service or a dedicated phone number/e-mail address for questions concerning this breach;
- Recommened measures to limit the negative effects of the breach, such as changing passwords.

The following general form can be used as a template for notifications. Evidently, it is wise to accompany this with letter containing an apology to data subjects in where one can also explain that Bedrijf Y B.V. has solved the breach and shall make all efforts necessary to prevent similar breaches in the future.

Notification data breach	
Description	On [DATE], a data breach has occurred which may have involved your data.
Questions	For questions, you can contact [NAME] at [EMAIL] or [PHONE NUMBER].
What can you do?	To limit the consequences of the breach, we recommend you to [MEASURES].

Notifications to the data subjects have to be made on an individual basis. For example, if customer data have been leaked, every customer must be informed separately. If a data breach is of such a considerable size meaning that a larger group is affected, then an e-mail can be sent to these perons, informing that a breach has occurred. The e-mail may contain a link to a web page providing more information on the breach. A single message in the media is not sufficient to inform the data subjects.

In principal, if those involved are to be informed, the notification should be made on an individual basis. Only if this is not feasible, due to the size of the group or the fact that it is not possible to trace which persons are and which persons are not affected by the breach, other ways to inform the data subjects may be considered.

7. Documentation of data breaches

When a data breach has been notified to the authority, a summary of the notification, as described in section 4, should be included in the administration. Under future privacy rules (the General Data Protection Act), which shall start to apply from 25 May 2018, all data breaches must be registered, even those that do not need to be notified. When there has been a data breach, whether or not it had to be notified to the authorities or data subjects, is must be documented by Bedrijf Y B.V. if it is the data controller in relation to this data breach.

Bedrijf Y B.V. may document the data breaches in a completely separate system, but this is not requires. It suffices to open a new file or dossier for the documentation of data breaches.

Reports sent to the authorities and data subjects in the context of the notification obligation must be stored by Bedrijf Y B.V.. When a data breach is not notified to the authorities or data subjects, the following information must be documented:

- the facts of the data breach;
- the consequences; and
- the correcting measures taken by Bedrijf Y B.V..

This register serves the following purposes:

- To learn a lesson from the data breach;
- To enable to answer questions from data subjects and third parties;
- To enable to notify data subjects, if this turns out to be necessary after all;
- To enable the monitoring of compliance with the obligation to notify (certain) data breaches to the authorities.

Example: Consider a database with personal data that has been publicly accessible for a short period of time, due to a hack. The data in this database were encrypted according to state of the art encryption standards, and thereby not unintelligible for persons without the required authorizations.

After half a year, it turns out that the used method of encryption has been superseded. In such case, the data subjects must be notified of the data breach that took place six months ago.

Please note: The administration does not have to be published, but the data protection authority must be provided access to it on its request.

8. Internal procedure for data breaches

8.1. Introduction

A data breach may occur within Bedrijf Y B.V. itself, but also within one of the third parties hired by Bedrijf Y B.V. (e.g. the supplier of a CRM system, the hosting provider, or a marketing agency). When a data breach occurs, it must be established where the data breach took place and how this breach must finally be notified to the authority and the data subjects.

Within Bedrijf Y B.V., this shall be initally the task of D. Atalek (Functionaris Gegevensbescherming). The contact details of D. Atalek are included in section 8.5.

It is important that all persons involved, including both the staff of Bedrijf Y B.V. and the staff of hired third parties, are able to identify a data breach. It is therefore very important to create awareness among the staff. The person who discovers the breach at all times needs to inform the above mentioned person about the breach.

8.2. Internal data breaches

When a data breach occurs within Bedrijf Y B.V., anyone within the organization should know how to act to enable a timely report to the right persons, and finally to the authority and data subjects. In such cases, the following procedure should be followed.

The breach is first discovered by someone, who can be anyone within Bedrijf Y B.V.. The discoverer reports the breach to D. Atalek (Functionaris Gegevensbescherming). D. Atalek shall then decide whether or not the data breach will be notified.

Registration
D. Atalek registers the report by the discoverer. The following details shall be registered:

- Who reported the discovery?
- What is reported?
- Where did the report come from?
- Which data are concerned?
- How did the breach occur (e.g. which data carrier has been lost)?
- Which system were involved in or affected by this incident?
- When did the breach take place?
- What has been done to solve the incident and/or prevent such incidents in the future?

Inform the board

Consquently, D. Atalek shall decide whether the breach will be notified to the authority and the data subjects. When the data breach has been notified to the authority and/or data subjects, D. Atalek shall take care of a correct internal administration of the data breach (see section 7). If Bedrijf Y B.V. is data processor and its customer is the data controller, it is important to check which arrangements on the notification of data breaches, occurring within the organization of the customer, have been made in the data processing agreement.

8.3. External data breaches

A data breach can also occur outisde of Bedrijf Y B.V., since personal data are also shared with third parties. For example, think of suppliers of software, or parties that deliver websites for Bedrijf Y B.V. or provide services for the storage of personal data. When a data breach occurs at a third party, this must be notified to Bedrijf Y B.V. as soon as possible. Third parties currently have a duty of care to report a data breach that they discover to Bedrijf Y B.V.. This duty is also explicitly mentioned in the GDPR.

Arrangement on this issue must be made in data processing agreements with these third parties. For each third party, Bedrijf Y B.V. must provide a contact in order to act swiftly on these notifications. This can be the same person that is the initial contact for security and data breaches within Bedrijf Y B.V., namely D. Atalek, or a contact from the third party in question that will subsequently report the data breach internally within Bedrijf Y B.V..

8.4. Notifying data subjects

If a data breach is known to Bedrijf Y B.V., it will need to establish how, if required, the data subjects (e.g. members) will be notified. In that regard, this response plan can be used as guidelines. When the third party, e.g. a customer, is the data controller and Bedrijf Y B.V. is a data processor, this party shall have to notify the data subjects, unless agreed otherwise with Bedrijf Y B.V..

8.5. Contact details

The following contact details are important if a data breach has occurred. At all times, contact D. Atalek directly.
The contact details are:
Functionaris Gegevensbescherming: D. Atalek, phone: 0209876543