AUTORITEIT
PERSOONSGEGEVENS

Questionnaire personal data breach notification form

In this document you will find the questions of the personal data breach notification form of the Autoriteit Persoonsgegevens (AP). This document will help you review the questions prior to filling out the online form. This way you can collect the necessary information in advance. In addition, the questionnaire can help your organization to draw up a step-by-step plan with which you can notify the AP of a (future) personal data breach as timely and complete as possible.

Version 1.0, September 2022

Disclaimer

No rights can be derived from this form. This form can be subject to change. The latest version can be found on the AP's website.

Please note: you cannot use this form to send a personal data breach notification to the AP via postal mail or email. The AP only accepts personal data breach notifications through the online notification form.

What information do you (possibly) need when notifying a personal data breach to the AP?

You will always need this information:

- contact details of the person who the AP can contact in case of questions;
- contact details of your Data Protection Officer (if applicable);
- correspondence on the discovery of the data breach;
- record of processing activities (Article 30 GDPR);
- personal data breach register (Article 33(5) GDPR);
- the measures taken to end the personal data breach;
- the measures taken to prevent the personal data breach in the future;
- the measures you had already taken before the personal data breach;
- data protection impact assessment (DPIA) (if applicable).

If there has been a hacking or malware incident, or any other incident in which (external) investigation has taken place:

- the investigation report following the personal data breach.

If you use a third party to process personal data:

- processing agreement;
- other agreements, e.g. cooperation agreements.

If you need to inform data subjects (affected individuals):

- correspondence to the data subjects.

Investigation for hacking, malware (e.g. ransomware) and/or phishing incidents

If you notify the AP of a personal data breach due to hacking, malware (e.g. ransomware) and/or phishing, the AP expects you to investigate or have an investigation performed into the extent of the incident as soon as possible. After all, malicious hackers may have applied malware and other changes to less visible parts of your network and/or systems, for example, allowing them to access your network at a later time. In addition, without investigation, you cannot get a conclusion as to whether personal data have been viewed, copied or stolen by third parties or has been changed. The AP expects you to include at least the following in your investigation:

- Has there been access to the personal data, for example to emails in a mailbox or the content of a database?
- Have these personal data been copied, accessed or otherwise transmitted to the hackers?
- Are there log data available and, if so, can you exclude from that log data that personal data have been copied or accessed?

Documentation obligation — Personal data breach register

Notifying a data breach to the AP is only part of the obligation to notify personal data breaches. In addition, you must keep a register in which you register all data breaches that occur within your organization. This includes the personal data breaches that you did not notify to the AP because that was not necessary. In any case, include in the register the following information:

- the facts about the personal data breach, such as the cause, what exactly happened and what personal data are involved;
- the consequences of the personal data breach;
- the measures you have taken to close the leak and to prevent recurrence.

It is recommended to also indicate why you notified, or did not notify, a personal data breach to the AP and the data subjects involved. This is not mandatory however.

AUTORITEIT
PERSOONSGEGEVENS

Questionnaire personal data breach notification Form

1. Introduction

Submitting a new notification of a personal data breach

1.1 What kind of notification do you want to submit?

- I want to notify one breach (regular notification) [= continue to 1.2]
- I would like to notify multiple similar breaches, as a result of a large-scale mail shipment, at the same time (bulk notification) [= continue to 1.1.2]

1.1.1. Has your organization received explicit written consent from the AP to notify breaches in bulk?

- Yes [=continue to 1.1.2]
- No [END FORM]

At the moment, there is a pilot in which only pension funds, insurers and banks are allowed to notify breaches in bulk. It is currently not possible to obtain permission to submit bulk notifications. As soon as it will be possible, it can be found on the AP's website.

1.1.2 Specify the number of breaches you want to notify to the AP in bulk:
[free field]

Under question 5.3 'Description of the incident', clearly indicate that this is a bulk notification, and indicate how many postal items are involved. Further, make sure that you have met all the conditions set by the AP for submitting a bulk notification before sending the notification.

1.2 Notification obligation GDPR, Tw, Wjsg or Wpg

On the basis of which legal provision do you submit this notification?

- General Data Protection Regulation (GDPR)
- Telecommunications Act (Tw)
- Law on Judicial and Criminal Data (Wjsg)
- Police Data Act (Wpg)

The obligation to notify personal data breaches is included in four laws. In most cases, you will make a notification under the GDPR. Only if you are a telecommunications provider or you process personal data on the basis of the Wjsg or the Wpg, this can be different.

1.3 Did your organization or company notify the breach to regulators of other notification obligations? Or are you going to do that?

- Yes, namely: Multiple options are possible.
- ☐ Financial Markets Authority (AFM)

- ☐ Telecom Agency (AT)
- ☐ The Dutch National Bank (DNB)
- ☐ Health and Youth Inspectorate (IGJ)
- ☐ Inspection Environment and Transport (ILT)
- ☐ Inspection for Education
- ☐ National Coordinator for Counterterrorism and Security (NCTV)
- ☐ Research Board for Security (OVV)
- ☐ Other regulator, namely [free field]

○ No

2. International aspects

2.1 Cross-border personal data breach

2.1.1 Does the personal data breach affect persons in several countries?

- Yes [= continue to 2.1.2]
- No [= continue to 3]

If you process personal data in more than one country or where the processing may have harmful consequences for individuals in more than one country, you may need to notify the breach to more than one supervisory authority. Are you unsure whether you should notify the breach to the AP or to a supervisory authority from another European country? Then you can use the Flowchart Identification Leading Supervisor (Dutch). See also the Q&A (Dutch) for more information.

2.1.2 Is the main establishment or the sole establishment of your organization located in the Netherlands?

- Yes [= continue to 2.1.3]
- No [= continue to 2.1.3]

The AP is the leading supervisory authority when the principal place of business or the sole establishment of your organization is located in the Netherlands.

2.1.3 In the case of cross-border data processing, which countries are concerned?

[list of EU countries + possibility to specify other countries + option to specify number of data subjects]

2.2 Competent supervisory authorities in other EU Member States

2.2.1 Did your organization notify the personal data breach to other privacy authorities?

- No [= continue to 2.2.2]
- Yes [= continue to 2.2.1.1]

2.2.1.1 Please indicate in which country(s) you have notified the breach to the privacy regulator. Multiple options are possible.

[list of EU countries + possibility to specify other countries + option to specify number of data subjects]

2.2.2 Will your organization notify the personal data breach to other privacy regulators?

- No [= continue to 3]
- Yes [= continue to 2.2.2.1]

2.2.2.1 Please indicate in which country(s) you are going to notify the personal data breach to the privacy regulator. Multiple options are possible.

[list of EU countries + possibility to specify other countries + option to specify number of data subjects]

3. Notifying organization

3.1 Contact details
3.1.1. Which organization or company is the notification about?

Registration number of the DPO	[free field] [optional]
Chamber of Commerce number	[free field] [optional]
Name of the company or organisation	[free field]
Address	[free field]
Postal code	[free field]
City	[free field]

3.1.2 In which sector does the organization or company operate?
[List of sectors]

If you are not sure in which sector you are active, check within which SBI you are registered with the Chamber of Commerce or select the sector closest to your economic activities.

3.2 Details reporter and contact person
3.2.1 Who reports the breach?

Name	[free field]
Function	[free field]
E-mail address	[free field]
Phone number	[free field]
Second phone number	[free field] [optional]

This should be a direct number and not a general phone number.

3.2.2 Is the reporting person the contact person whom the Dutch Data Protection Authority can contact for further information about the notification?

- Yes [= forward to 3.3]
- No [insert fields and then proceed to 3.3]

Name	[free field]
Function	[free field]
E-mail address	[free field]
Phone number	[free field]
Second phone number	[free field] [optional]

The contact person must be easy to reach during office hours the day after the notification in order to be able to answer any questions of the AP about the breach.

3.3 Other organizations

3.3.1 Were there any other organizations involved in the breach?

- Yes [= forward to 3.3.2]
- No [= forward to 4]

An organization is involved in the breach if it has had a role in the occurrence of the breach.

3.3.2 Specify which other organizations were involved in the breach?

Name	**In what way involved**	**Explanation (optional)**
Organization A	for example processor	
Organization B		
+ Add another organization		

4. Timeline

4.1. Is the personal data breach still ongoing at this time?

- Yes [=continue to 4.1.1]
- No [=continue to 4.1.1 + 4.1.2]
- Unknown [=continue to 4.1.1]

4.1.1 (Possible) start date of the breach
[date field]
4.1.2 (Possible) end date of the breach
[date field]

4.2 When was the incident discovered?
[date field]

4.3 Indicate (shortly) how you discovered the breach
[free field]

4.4 Is the moment when you discovered the incident also the moment when you labeled the incident as a breach ('data breach') and thus became aware of the breach?

- Yes [=continue to 5, unless later than 72 hours after the date of discovery then forward to 4.5]
- No [=continue to 4.4.1]

By gaining awareness of a personal data breach, it is meant that you have been able to assume, based on objective factors, that it is likely that a personal data breach has occurred. This does not have to be the time when you discovered the data breach. **Please note**: This cannot be the time when the incident was reported to the DPO. The DPO is not responsible for the obligations that the data breaches notification obligation entails. This means that the AP does not consider this as a justified reason why the notification was submitted too late.

4.4.1 When did you become aware of the breach?
[date field]

If the breach is notified later than 72 hours after having become aware of it, the following question must be answered:

4.5 Describe below why you notify the breach later than 72 hours after discovery:
[free field]

5. Information about the breach

5.1 Nature of the breach Multiple options are possible.

An incident may involve one or more types of breaches relating to the confidentiality, availability and integrity of the personal data. An example of this is when you are confronted with ransomware. In order to encrypt/ransom a file, the malicious software must first open the files before encrypting them. As a result, there is a breach of confidentiality/viewed by unauthorized persons as well as a breach of availability. For more information, see our Q&A (Dutch).

- ☐ Personal data (possibly) viewed by unauthorized persons

The term 'viewed' also refers to unauthorized or unintentional sending of or access to personal data.

- ☐ Personal data have been changed unauthorized or unintentionally
- ☐ Personal data permanently unavailable (lost/deleted)
- ☐ Personal data temporarily unavailable

This should involve accidental or unauthorized loss of access to personal data or an accidental or unauthorized destruction of personal data. This may also apply if you cannot (temporarily) use the personal data necessary for the processing purposes.

5.2 Nature of the incident
What is the nature of the incident where there has been a personal date security breach? Only one option is possible.

- ☐ Email with personal data sent to the wrong recipient(s)
  5.2.1.Has the wrong recipient confirmed to have deleted the email?
  - Yes [= continue to 5.3]
  - No [= continue to 5.3]
  - The wrong recipient did not respond [= continue to 5.3]
- ☐ Email sent with personal data with recipients in the 'to'-field or in the cc, instead of bcc [= continue to 5.3]
- ☐ Letter or postal package containing personal data sent or delivered to the wrong recipient(s)
  5.2.2. Has the wrong recipient confirmed that the personal data have been destroyed, or have the personal data been returned?
  - Yes [= continue to 5.3]
  - No [= continue to 5.3]
  - The wrong recipient did not respond [= continue to 5.3]

- ☐ Received back an opened letter or postal package containing personal data [= forward to 5.3]
- ☐ Lost letter or postal package containing personal data [= forward to 5.3]
- ☐ Authorizations(s) of employee(s) set incorrectly. [= continue to 5.3]

This incident relates to the situation where a user's access or reading rights have not been modified or have been erroneously altered, giving a user more possibilities in the system than it should. For example: an authorization role is not implemented properly in the event of a change of function.

- ☐ Network folders or locations with personal data are too widely accessible within the organization. [= continue to 5.3]

This refers to the system, where a shared folder, location or application is incorrectly set up and can therefore be viewed by unauthorized persons. For example: A folder with staff data was accessible to every employee.

- ☐ Device, data carrier (e.g. USB stick) and/or paper containing personal data is lost or stolen [= continue to 5.3]
- ☐ Personal data accidentally published [= continue to 5.3]
- ☐ Hacking, malware (e.g. ransomware) and/or phishing Multiple options are possible

The AP also advises you to report to the Police for, among other things, hacking and/or computer sabotage. By submitting a report, the police, in consultation with the Public Prosecutor's Office (OM), can decide to start an investigation and help the OM to identify crime. This allows the police to detect criminal offences and prevent more victims. For more information, please visit www.nomoreransom.org.

- ☐ Phishing [= forward to 5.2.3]

Phishing is a collective name for digital activities that aim to extract information from people. This information allows criminals to access (business) networks and commit fraud, e.g. bank fraud or identity fraud.

- ☐ Ransomware [= continue to 5.2.3]

Ransomware is malicious software that hostages a computer or files. In most cases, payment is demanded.

- ☐ Other types of hacking and/or malware [= continue to 5.2.3]

This may include all activities in which unauthorized access to personal data has been granted or in which personal data are otherwise unlawfully affected.

5.2.3. Have you conducted (digital forensic) investigation into the nature and extent of the breach? [= forward to 5.3]

- Ransomware can hit the entire system and all linked files. In case of ransomware, without conducting (digital forensic) investigations, you cannot assume that the breach has been limited to the visibly infected file or system.
- A successful phishing action, where an email address and a password have been obtained, can lead hackers to access mailboxes, networks and systems. In the case of mailboxes, it is possible that the e-mails in a mailbox are also affected. In the case of phishing, not only the contacts in the address book of the email account may be affected, but also the persons whose emails are stored in the mailbox.

- o Yes, the investigation is ongoing

Once the investigation is completed, you must submit a follow-up notification to the AP.
The AP expects you to include at least the following in your investigation:

- Has there been access to personal data, for example to emails in a mailbox or the content of a database?
- Have these personal data been copied, accessed or otherwise transmitted to the hackers?
- Are there log data available and, if so, can you exclude from that log data that personal data have been copied or accessed?

- o Yes, the investigation has been completed [= continue to 5.2.3.1]

5.2.3.1. Upload the report of the investigation into the breach here
[UPLOAD button] [optional]

- o No, the investigation has not started yet.

The AP expects you to investigate the nature and extent of the breach as soon as possible. You must submit a follow-up notification within 4 weeks with the state of affairs. The AP expects you to include at least the following in your investigation:
- Has there been access to personal data, for example to emails in a mailbox or the content of a database?
- Have these personal data been copied, accessed or otherwise transmitted to the hackers?
- Are log data available and, if so, can you exclude from that log data that personal data have been copied or accessed?

- No, no research is being conducted

Without an investigation, uncertainty about the extent of the breach will remain. This means that you cannot reasonably exclude that personal data has been viewed, copied, stolen or altered by a third party. The AP expects you to investigate the nature and extent of the breach as soon as possible. The AP expects you to include at least the following in your investigation:
- Has there been access to the personal data, for example to emails in a mailbox or the content of a database?
- Have these personal data been copied, accessed or otherwise transmitted to the hackers?
- Are log data available and, if so, can you exclude from that log data that personal data have been copied or accessed?

5.2.3.2 Explain why you are not conducting an investigation.
[free field]

- ☐ Personal data of the wrong customer shown in customer portal
- ☐ Personal data added to the wrong file
- ☐ Personal data added to paper waste
- ☐ Personal data due to malfunction (temporarily) not available
- ☐ Other, namely: [free field]

5.3 Description of the incident
Provide a summary of the incident where there has been a personal data security breach
[free field]

5. 4 If available: upload relevant supporting documentation to your notification here Please note: do not include personal data in the files if this is not necessary.
[Upload button] [optional]

6. Personal data involved

6.1 Personal data in general Multiple options are possible

- ☐ Name
- ☐ Sex
- ☐ Date of birth and/or age
- ☐ Social security number (BSN)
- ☐ Contact details
  - ☐ Address and place of residence
  - ☐ E-mail address
  - ☐ Phone number
- ☐ Access or identification data

For example usernames and passwords.

- ☐ Financial data
  - ☐ Bank account number/IBAN
  - ☐ Credit card details
  - ☐ Data on (problematic) debts
  - ☐ Data on benefits and/or debts
  - ☐ Other financial data, namely: [free field]
- ☐ (Copies of) passports or other proofs of identity
- ☐ Location data

No address information. This means data to determine or be able to track a person's location, e.g. GPS data, transmission tower data.

- ☐ Personal data relating to criminal convictions and criminal offences or related security measures

Also indirectly, data may be considered criminal offence personal data, e.g. derived from the design or logo of an envelope originating from the probation office or the Public Prosecutor's Office.

- ☐ Other, namely: [free field]
- ☐ Unknown

If unknown is selected:
You must submit a follow-up notification within 4 weeks, in which you indicate which personal data are involved in the data breach.

6.2 Special categories of personal data

A special category of personal data may also be indirectly apparent from facts and circumstances of the situation. Think, for example, of the envelope used or the special feature of your organisation, for example a church, trade union, LGBTQ association, a mental health institution or specialist care (e.g. oncology).

- ☐ Personal data revealing a person's racial or ethnic origin
- ☐ Personal data revealing a person's political views
- ☐ Personal data revealing a person's religious or philosophical beliefs
- ☐ Personal data revealing a person's membership of a trade union
- ☐ Data relating to a person's sexual behavior or sexual orientation
- ☐ Data on a person's health
- ☐ Genetic data
- ☐ Biometric data (for example: fingerprint or iris scan)

These are personal data resulting from a specific technical processing of a person's physical, physiological or behavioural characteristics. Based on this data, unambiguous identification of that person is possible. Or his/her identity will be confirmed.

6.3 Quantity of personal data
6.3.1 Specify (approximately) how many data records (data registers) were affected by the breach
[free field]

A data record (Article 33(3)(a) GDPR) means: the recording of information about an event or about a person. The concept is best explained through examples:

1) Each row in a database forms a single data record. This can be a database with all orders placed, but can also be a database with all customer data (CRM). 100 customers in a CRM system are 100 records. If each customer has placed 5 orders with that company, there are 500 data records included as an order in the order database.
2) Each row in a log forms a single data record. For example, a medical file keeps track of who has been inspected and has carried out actions in the file. If someone has opened a file and has modified one thing, at least three lines may have been created (open file (1), change information (2), close file (3)).
3) A letter constitutes a single data record. The date, details of the addressee and sender shall be contained as information in the letter.
4) An email is a single data record. The date and time of dispatch, the consignee and the sender are in the mail.
5) A passport is a single data record. A passport contains information about a person, such as name, date of birth, nationality, BSN, passport

document number and customs stamps of the countries where someone has been.

6) A (paper) file of a person is also a record, because information is stored on there about a person.

It is possible that multiple types of data records have been affected in the event of a breach, because, for example, the entire network has been affected, which affects both CRM and HR data. In the next question, you can provide an explanation of the affected data records. If the number of data records is too large or if you do not know how many personal data registers have been affected, enter '1' and explain the number in the next question. For more information, see the Q&A (Dutch).

Please explain the above number:
[free field]

Here you can provide a more detailed explanation of the number and type of affected data records. Based on your explanation, the AP can get a better or more nuanced picture of the incident. For example, you can indicate whether one or more databases have been affected or whether the infringement is limited to a letter or file.

7. Affected individuals

7.1 Which group(s) of data subjects were affected by the breach?
Multiple options are possible.

- ☐ Employees
- ☐ Customers (current and potential)
- ☐ Students
- ☐ Patients
- ☐ Minors
- ☐ Persons from other vulnerable groups
- ☐ Otherwise, namely: [free field]

'Data subject' refers to the person whose personal data have been affected by the breach in this context.

7. 2 Give a more detailed description of the group(s) involved.
[free field]

7. 3 Is the exact number of data subjects involved known?

- ☐ Yes
  7.3.1 The exact number is:
  [free field]

- ☐ No
  7.3.2 The minimum number of data subjects involved is:
  [free field]
  7.3.3 The maximum number of data subjects involved is:
  [free field]

8. Measures taken before the breach

8.1 Were the personal data encrypted, hashed or otherwise rendered incomprehensible or inaccessible to unauthorized persons before the breach occurred? Multiple options are possible.

☐ Yes, namely: encrypted
8.1.1 What encryption technique have you used (if known)? [open field+ optional]

If possible, try to provide details such as the number of bits of the key used and the standard (e.g. AES-256). Please note: if a laptop or other carrier is password-protected, this does not always mean that the data on the carrier are encrypted and 'encrypted' does not mean: encrypted by a ransomware attack.

☐ Yes, namely: hashed
8.1.2 What hashing technique have you used (if known)? [open field+ optional]

For example, think of MD5, SHA-256, bcrypt, or some other cryptographic hash function. Please indicate whether a salt has been used.

☐ Yes, namely: otherwise rendered incomprehensible or inaccessible
8.1.3 How were the data made incomprehensible or inaccessible (if known)?
[open field+ optional]

Think of standard encrypted soft- or hardware or other security methods

☐ No [= direct to 9]

8.2 If the personal data were made incomprehensible or inaccessible, which part does it concern?

- ○ All data were previously incomprehensible or rendered inaccessible.
- ○ Some of the data were rendered incomprehensible or inaccessible, namely: [free field]

9. Consequences

9.1 (Possible) consequences for the controller and the personal data.
Multiple options are possible.

- ☐ Unauthorized persons have been able to take note of the data
- ☐ The data may be used in an improper or unlawful manner
- ☐ Incorrect, incomplete or outdated personal data may be used within your own organization
- ☐ Incorrect, incomplete or outdated personal data may be reused for other purposes or transferred to other organizations
- ☐ An essential service can no longer be provided temporarily to those whose data have been leaked
- ☐ An essential service can no longer be provided permanently to those whose data have been leaked
- ☐ Otherwise, namely: [free field]

This means the possible impact of the breach on your organization and the processing of personal data within your organization.

9.2 (Possible) consequences for the data subject(s) Multiple options are possible.

- ☐ Discrimination or exclusion
- ☐ Identity theft or fraud
- ☐ Financial loss
- ☐ Reputational damage
- ☐ Loss of confidentiality of personal data protected by professional secrecy
- ☐ Unauthorized undoing of pseudonymisation
- ☐ For example, data subjects cannot access (the processing of) their personal data or have them deleted upon request (Exercise of rights)
- ☐ Data subjects lose the overview of which organizations process their personal data and are prevented from exercising control
- ☐ Other, namely: [free field]

9.3 Estimation of risk
Please provide an estimate of the severity of the possible consequences for the data subject(s)

- ○ Negligible
- ○ Limited
- ○ Significant
- ○ Very large

Please explain your choice:
[free field]

There are at least 7 factors to take into account:

1. What incident happened?
2. How much personal data and what type of personal data have been affected and how sensitive are the personal data in the context in which the personal data are processed?
3. How easy is it to link the data to a natural person?
4. How serious can the consequences indicated above be?
5. Does the data subject belong to a vulnerable group?
6. Does your organization have a special position (such as a hospital, a bank, a (special) school)?
7. What is the size of the group involved?

In addition, you can take into account specific facts and circumstances that increase or reduce the risk for data subjects. For more information, see the Guidelines on Personal data breach notification, starting from page 27.

10. Measures taken after the breach

10.1 Informing data subject(s)

10.1.1 Have you already communicated the breach to the data subject(s)?

- Yes [= continue to 10.1.3]
- No [= continue to 10.1.2]

10.1.2 Do you plan on communicating the breach to the data subjects?

- Yes [= continue to 10.1.4]
- No [directly continue to 10.2]
- Not yet known [directly continue to 10.2]

Please note, you must assume that you must communicate the breach to the data subject(s) in relation to the following personal data:

- special categories of personal data
- criminal personal data
- copies of identity documents and/or passports
- combination of BSN, name and date of birth
- personal data of a vulnerable group
- many personal data or personal data of many data subjects

And/or the breach may lead to:

- discrimination
- identity theft or fraud
- financial losses
- reputational damage
- breach of professional secrecy

See also: Guidelines on Personal data breach notification

Pay attention to phishing
If you notify a phishing incident regarding an email account, you may need to inform two groups of data subjects, namely those whose contact details were in the address book in the email box and those whose (special or sensitive) personal data were stored in emails in the email box, for example in an attachment.

10.1.3 How many data subjects did you communicate the breach to?
[input field]

10.1.4 How many data subjects do you want to communicate the breach to?
[input field]

Please note: does the number of data subjects that you are going to inform not correspond to the number you specified in question 7? Then we ask you to explain this in more detail.

Pay attention to phishing
If you notify a phishing incident regarding an email account, you may need to inform two groups of data subjects, namely those whose contact details were in the email box and those whose (special or sensitive) personal data were included in emails in the email box, for example in an attachment.

10.1.5 When did you notify the data subject(s) about the breach? [= forward to 10.1.7] [date field]

10.1.6 When do you (expected) to notify the data subject(s) about the breach? [= forward to 10.1.7]
[date field]

10.1.7 Please explain which (group of) data subjects you have notified about the breach. [= forward to 10.1.8] [free field]

10.1.8 What is the content of the notification to the data subject(s)? [= forward to 10.1.9] [free field]

You are obligated to indicate:
- what happened;
- what the consequences are;
- what measures you have taken, and;
- the name and contact details of the Data Protection Officer or any other contact point from which more information can be obtained.

Optional: Upload a copy of the text of this notice here [UPLOAD button]

10.1.9 What/which means of communication do you use or intend to use to notify the data subject(s)? Multiple options are possible.
- ☐ By phone
- ☐ By letter
- ☐ By email
- ☐ Via a notice on the website
- ☐ Via social media
- ☐ Through an advertisement in the newspaper
- ☐ Otherwise, namely: [free field]

If only 'Via a notice on the website' is ticked:
A notice that is limited to a general notice on your website is generally not an effective means of communicating a breach to any person. The AP recommends that you choose a means where the chance that the information will be properly communicated to all affected persons is as high as possible. This can mean that you use different communication methods instead of a single contact channel. For example, via an additional press release, your company blog, and via your organization's official social media accounts.

10.2 Reason not to (personally) inform the data subject(s)
10.2.1 Why do you refrain from notifying (part of) the persons whose data were affected by the breach about the incident? Multiple options are possible

- ☐ It would involve a disproportionate effort to inform each person on an individual basis
  10.2.1.1 Explain why it would involve a disproportionate effort to inform the data subjects on an individual basis. [free field]
- ☐ The measures I took before the breach took place provide sufficient protection to avoid communicating to the data subject(s)
  10.2.1.2. What measures have you taken so that it is not necessary to inform the data subjects? [free field]
- ☐ After the breach, I have taken measures that make it no longer likely that there will actually be a high risk to the rights and freedoms of the data subject(s)
  10.2.1.2. What measures have you taken so that it is not necessary to inform the data subjects? [free field]
- ☐ My organization is a financial undertaking as referred to in the Financial Supervision Act (exception under Article 42 UAVG)
- ☐ There is an overriding interest not to inform the affected persons, namely: [free field]

The affected persons need not be informed, where necessary and proportionate in order to protect:
- national security;
- national defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and the prevention of threats to public security;
- other important objectives of general interest of the European Union or of the Netherlands, in particular an important economic or financial interest of the European Union or of the Netherlands, including monetary, budgetary and fiscal matters, public health and social security;

- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of violations of professional codes for regulated professions;
- a supervisory, inspection or regulatory task relating, even occasionally, to the exercise of official authority in the cases referred to in subparagraphs (a), (b), (c), (d), (e) and (g);
- the protection of the data subject or the rights and freedoms of others; or the recovery of civil claims.

- Other reason(s), namely:
  [free field]

10.3 Measures to address the breach

10.3.1 Has your organization taken measures to address the breach?

- No, because:
  [free field]
- Not yet known [You are obligated to provide a follow-up notification indicating what measures you have taken to end the breach.]
- Yes, namely:
  [free field]

For example, requested the destruction of the incorrectly delivered letter or deletion of the email, checking the logging to rule out a breach, closing the security breach, adjusting the authorisation structure/rights structure.

10.4 Has your organization taken measures to prevent new similar breaches in the future?

- No, because:
  [free field]
- Not yet known [You are required to provide a follow-up notification indicating what measures you have taken to prevent new similar breaches.]
- Yes, namely:
  [free field]

For example, providing awareness training, adjusting work processes, applying encryption to mobile data carriers such as laptops and USB sticks, or implementing two- or multifactor authentication (MFA) on email accounts or applications.

11. Submit

Is this a preliminary or a final notification?

- Yes, the notification is final. I have provided the required information and no follow-up notification is required.
- No, the notification is preliminary. There will later be a follow-up notification with additional information about the breach.

Are you still investigating the nature and extent of the breach? Then the AP asks you to fill in 'no' here and to submit a follow-up notification within 4 weeks in which you inform the AP of the progress or outcome of the investigation.

Date of follow-up notification later than 4 weeks:
Indicate when you submit a follow-up notification (at the latest).
[date field]

The AP will ask you to submit a follow-up notification within 4 weeks of the first notification in which you provide an update on the state of affairs. If you need more than 4 weeks, you need to justify this.

Did the AP not receive a follow-up notification within 4 weeks? Then the AP can contact you. If you do not submit a final notification, you cannot (completely) have complied with your notification obligation pursuant to Article 33 GDPR. The AP can then conduct a further investigation.

- ☐ By ticking this box, you declare to have filled in this form truthfully.
- ☐ By ticking this box, you declare that you are authorized to make this notification on behalf of your organization.

Privacy statement

- ☐ I am aware of the content of de Privacy Statement of the AP

END OF FORM