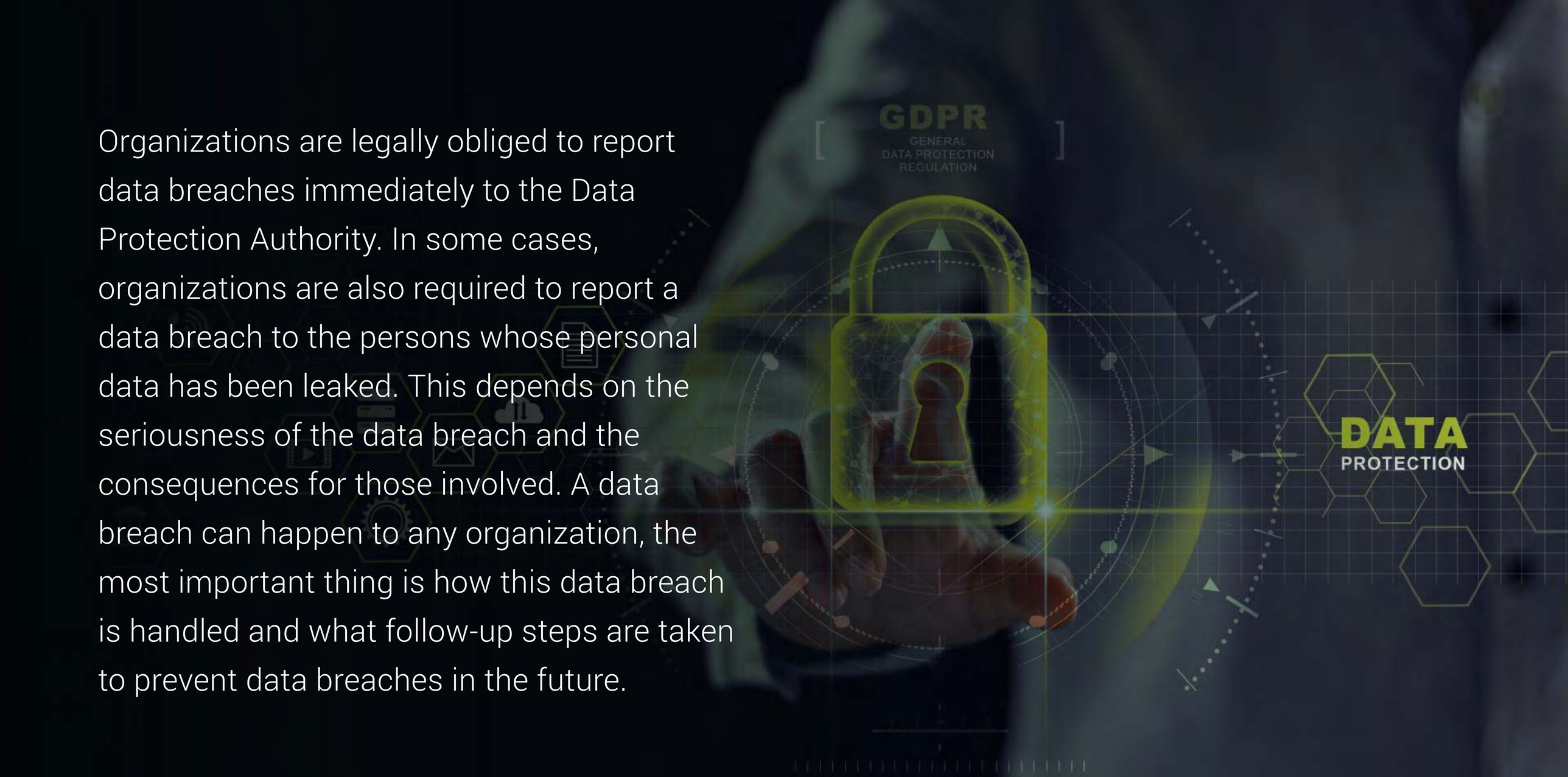
TOOLKIT

# Step-by-step plan data breach protocol

DPO Consultancy
Experts in Data Privacy

MAY 2021

Organizations are legally obliged to report data breaches immediately to the Data Protection Authority. In some cases, organizations are also required to report a data breach to the persons whose personal data has been leaked. This depends on the seriousness of the data breach and the consequences for those involved. A data breach can happen to any organization, the most important thing is how this data breach is handled and what follow-up steps are taken to prevent data breaches in the future.



# What is a data breach?

A data breach is a breach of the security of personal data according to the General Data Protection Regulation (GDPR). Personal data is data that can be directly or indirectly traced back to a person. We speak of a data breach if personal data is lost, destroyed, or changed without the intention of an organization, or if unauthorized persons gain access to personal data.

Examples of data breaches are:

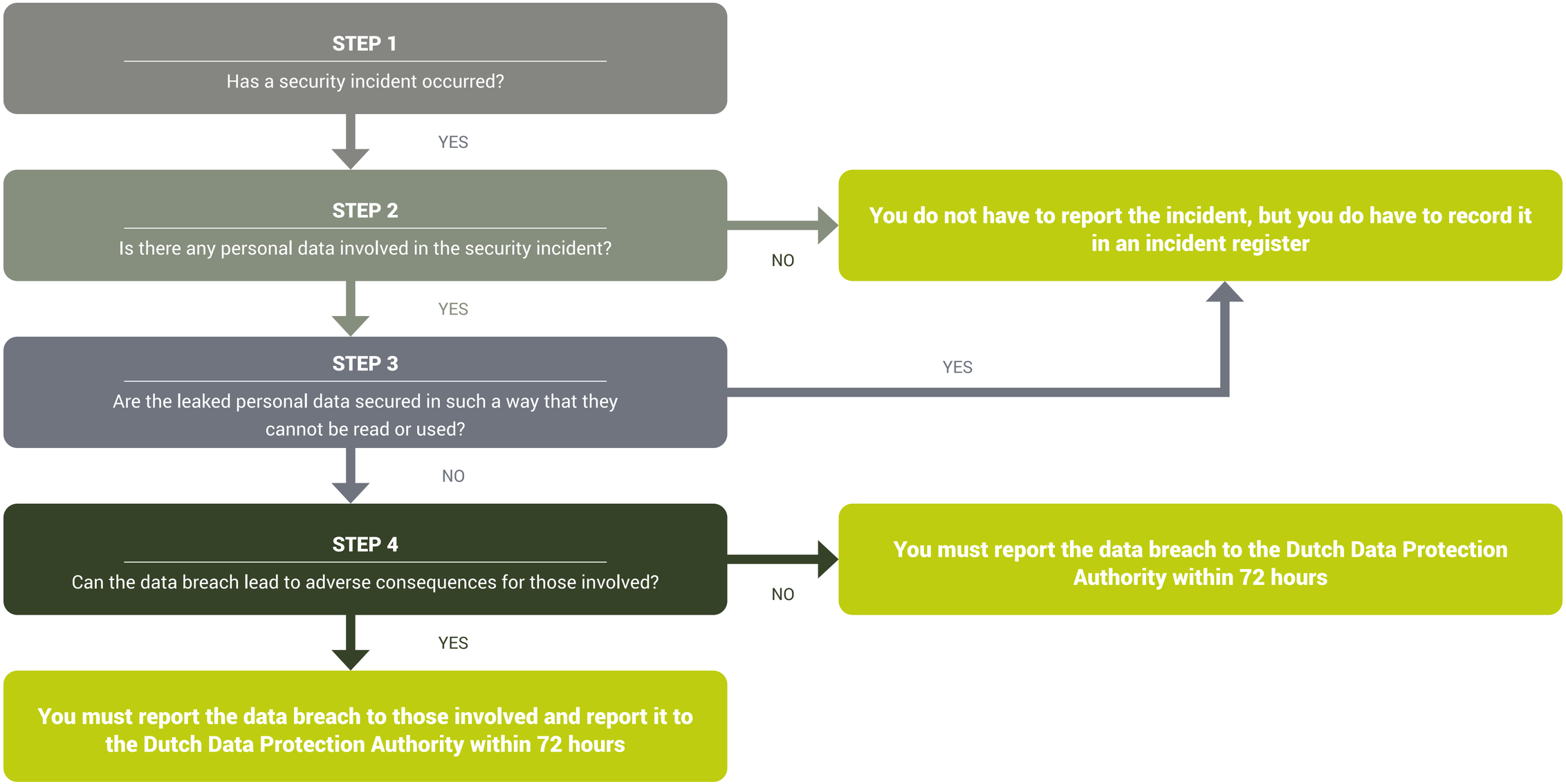
- A lost USB stick with personal data on it
- A stolen work laptop, tablet, or mobile phone without encryption;
- A break-in by a hacker
- Sending an email in which the email addresses of all recipients are visible to all other recipients;
- An infection with ransomware
- Providing personal data to an unauthorized person outside the organization
- Paper documents with personal data that end up on the street
- A vulnerability in an application through which personal data can be seen by all users

# Data breach protocol

In the event of a data breach, it is important as an organization to know which steps to take, when to do so and to whom to report a data breach. Those steps are described in a data breach protocol. The purpose of a data breach protocol is to deal with the consequences of a data breach in a controlled manner. It is a plan with which organizations can determine whether a data breach should be reported, how this should be done, and who fulfills which role if there is a data breach.

With this step-by-step plan, we help your organization to set up a data breach protocol. We explain which procedures must be included in the protocol and which steps you must follow. That way you always keep control over the situation.

“Passwords are like underwear: don’t let people see it, change it very often, and you shouldn’t share it with strangers.” Chris Pirillo


STEP 1
Has a security incident occurred?
YES
STEP 2
Is there any personal data involved in the security incident?
NO
You do not have to report the incident, but you do have to record it in an incident register
YES
STEP 3
Are the leaked personal data secured in such a way that they cannot be read or used?
YES
NO
STEP 4
Can the data breach lead to adverse consequences for those involved?
NO
You must report the data breach to the Dutch Data Protection Authority within 72 hours
YES
You must report the data breach to those involved and report it to the Dutch Data Protection Authority within 72 hours

# The steps of the data breach protocol

The data breach protocol includes various steps that an organization must go through if a data breach is discovered. To help you draw up a protocol, the flowchart below lists the various questions that you as an organization must answer in the event of a data breach. We provide an explanation for each question, giving you all the information you need to set up a data breach protocol for your organization.

STEP 1

### Has a security incident occurred?

As an organization, you try to protect the personal data you store as well as possible. But sometimes something goes wrong. For example, you no longer have access to your data or outsiders get access unintentionally. Then there is a security incident. A security incident is an event where there is the possibility that the confidentiality, integrity, or availability of information or information processing systems is or could be compromised.

STEP 2

### Is personal data also involved in the security incident?

A data breach exists if, due to a breach of security or other incident, the confidentiality, integrity, and/or availability of personal data cannot be guaranteed. For example, if the leaked data contains names, e-mail addresses, address details, or social security numbers. Not every security incident immediately leads to a data breach. If there is no data breach, record this incident in an internal incident register. Every organization is obliged to keep such an incident register. This records which incidents have taken place. The purpose of this register is to learn from previous incidents and take measures to reduce the chance of new data leaks. In addition, this register helps your organization to comply with the accountability obligation included in the GDPR. The Dutch Data Protection Authority may request that this register be shared.

**Data breach reporting obligation**
If there is a data breach, you as an organization want to know when and how to report the data breach. To this end, we make a distinction between the duty to report to the Dutch Data Protection Authority and the duty to report to those involved.

STEP 3

### Is the leaked personal data secured in such a way that they cannot be read or used?

If the information is anonymized, pseudonymized, or otherwise encrypted by the organization, it may not be a data breach. For example, a secured lost USB stick with personal data is not a data leak, because the data on the USB stick cannot be consulted without the decryption key. The standard that you must apply for this is very strict. Data may only be considered incomprehensible or inaccessible if it meets one of the following conditions:

- The data is securely encrypted with an algorithm. The decryption key is not compromised by any breach and is generated in such a way that people without authorized access cannot find the key - with the available technological means.
- The data has been replaced with hash values, which are cryptographically encrypted with a hash function. The key used for this is not compromised by any breach and is generated in such a way that persons without authorized access cannot find the key with the available technological means.

In addition to encryption, the remote erasure of data on a device (remote wiping) is also referred to as a technical protection measure for personal data. However, a number of preconditions must be met for this.

- The remote wipe is set in motion on time so that unauthorized persons have no chance to access the data.
- The device whose data is being deleted must still be intact and working for the remote wipe to be performed.
- The data erasure application must work properly so that all personal data is effectively deleted and no traces are left with which to reconstruct the original data.

If the incident leads to an incident with personal data, the leak must be reported to the Dutch Data Protection Authority within 72 hours after the organization has become aware of the data breach.

**STEP 4**

## Can the data breach lead to adverse consequences for those involved?

The data breach must be reported to data subjects if the breach is likely to pose a high risk to the rights and freedoms of data subjects. The damage can be physical, material, or immaterial. For example, physical damage involves the deletion of medical data, which prevents someone from receiving the necessary care. In the event of material damage, there is a chance that someone will suffer financial loss or become the victim of identity fraud. And in the case of immaterial damage, it concerns, for example, unlawful publication, damage to honor and reputation, or discrimination.

With personal data of a sensitive nature (also known as special categories of personal data according to the GDPR), the risk that the rights and freedoms of the data subjects are violated is much higher. For example, loss or unlawful processing can lead to, among other things, stigmatization, exclusion, damage to health, financial damage, or (identity) fraud of those involved. Examples of special categories of personal data are:

- Information about a person's religion or belief, race, political affiliation, health, sexual orientation, or memberships.
- Criminal personal data. Consider, for example, an area ban or traffic fines.
- Financial or economic data about debt, salary, and payment data.
- Data about, for example, addictions, school or work performance, or relationship problems could lead to stigmatization or exclusion of people.
- Usernames, passwords, and other credentials. The possible consequences depend on what the login details provide access to. Bearing in mind that many people reuse passwords for different accounts.

- Data that can be misused for (identity) fraud. This includes biometric data, copies of identity documents, and social security numbers.

The size and nature of the data breach can also lead to serious adverse consequences for the data subject. Data leaks at government institutions, banks, or insurers can, among other things, lead to financial damage for those involved. That is why, as an organization, you must also determine whether a data breach has serious adverse consequences for people or whether the chance of serious consequences has increased significantly. The following matters are relevant here:

- In the event of a data breach, it must always be determined how attractive the data is to abuse. If personal data is leaked from large groups of vulnerable people or multiple data from one individual – such as a public figure – the chance that data will be misused or resold increases. As a result, those involved may suffer from the data breach in the long term.
- If an organization processes personal data to make decisions that affect the data subjects, the risk on the rights and freedoms of those data subjects also increases. For example, if an organization uses financial personal data to determine a person's creditworthiness, the consequences of loss and unlawful processing of the data are more drastic than when using personal data for marketing purposes.
- In the government, personal data is often shared between different authorities, which means that a data breach can have consequences at various places in the chain. This makes it more difficult for data subjects to oversee the possible consequences of a data breach and to protect themselves against it.

If the nature and extent of the data breach meet one of the above criteria, there is a considerable chance that the data breach will have serious adverse consequences for those involved.

Based on the criteria from step 4, your organization can estimate whether the parties involved should be informed about the data breach. It is not an easy issue, because the impact of a data breach can (almost) never be compared with other data breaches. As an organization, you really have to look carefully at the possible impact that the data breach has on the lives of those involved. Therefore, treat each data breach as a unique event and assess (also record this in writing) per incident whether a report must be made to the parties involved.

## Getting started

By following the steps above, you as an organization are able to set up a data breach protocol yourself. In addition to drafting, the implementation of the protocol is of great importance, so that all parties involved know what is expected of them in the event of a security incident.

**Are you not quite sure, or do you have additional questions about specific topics? Please contact us via info@dpoconsultancy.nl or +31 85 0711080**

Australiëlaan 12a
5232 BB 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

1 Lyric Square London
W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com