|  |
| --- |
|  **Guide to using Wired Relations' templates**  |

Wired Relations' templates\* can be used directly in your work with data protection and information security - but can also be used as inspiration for your own material. You can modify them as needed to make them exactly as you want them.

NOTE! There may be sections that are not relevant to all organizations. If this is the case, it will be clearly indicated in the text.

There will be places in the text where you are prompted to insert the organization's name or other information. In these cases, it will be marked as follows: [insert organization's name].

At the bottom of each document, there will be a table that provides an overview of the document's version, the latest update, and who is responsible for the document.

Here are some additional tips for using Wired Relations' templates:

* Read the instructions carefully before you start using the templates. This will help you understand how to use them effectively.
* Customize the templates to fit your organization's needs. You can add or remove sections, change the wording, and add your own logo and branding.
* Keep your templates up to date. Data protection and information security regulations are constantly changing, so it's important to make sure your templates are always up to date.

We hope you find Wired Relations' templates helpful. If you have any questions, please don't hesitate to contact us.

Here are some links to additional resources that you may find helpful:

* The Danish Data Protection Agency: <https://datatilsynet.dk/>
* The Danish Centre for Cybersecurity:  [Center for Cybersikkerhed (cfcs.dk)](https://www.cfcs.dk/da/)

**Policy for the handling of personal data breaches**

**1. Purpose**

This policy describes what a personal data breach is, and how a personal data breach is to be managed in [insert organization’s name here].

**2. Field of application**

All employees of [insert organization’s name here] are expected to be familiar with **point 1, 2, 3** and **4** of this policy, which describes what a personal data breach is, and what employees need to do in case of personal data breaches.

The compliance team of [insert organization’s name here] is expected to be familiar with the entire policy, as **point 5, 6** and **7** determine the procedures for the mandatory assessments, registrations, notifications and evaluations, etc. for the documentation required, which relate to personal data breaches.

**3. Definition of personal data breaches**

A personal data breach is defined by:

”*a security breach that leads to accidental or illegal destruction, loss, change or unauthorised transferring of or access to personal data that is transmitted, stored or otherwise processed*.”

A personal data breach can e.g. happen when:

* someone unauthorised can access personal data, e.g. someone other than the person/persons at the data controller that are authorised to access the personal data (the unauthorised party can both be external or internal in relation to the data controller).
* personal data is deleted or changed (even if it was an accident).
* someone unauthorised have hacked their way into the data controller’s systems and thereby had access to personal data.
* personal data have been transferred to someone unauthorised (whether intended or not).

Employees of [insert organization’s name here] will receive awareness training regarding the prevention and identification of personal data breaches in accordance with [insert organization’s name here]’s *information security policy*, and the guidelines, policies and procedures resulting therefrom.

**4. The employee’s reaction to a personal data breach**

If you discover a personal data breach, or if you suspect that a personal data breach has happened, it’s important you react immediately. The faster the reaction, the quicker the breach can be stopped (or avoided entirely), and in this way any possible risks and consequences may be reduced.

When you discover a personal data breach, you must proceed as follows.

Get an overview

*What’s happened?*

You need to identify and describe all possible details. You must gain an overview of what’s happened, including what categories of data subjects and categories of personal data that are affected by the breach and what the extend of the breach is.

By doing so, you’re better prepared for the next step of the process.

Stop/limit the breach to the extend possible

*Can the breach be stopped or limited?*

If it’s an ongoing personal data breach, it’s important to stop/limit the breach so that the possible consequences for the data subject are minimised. It may be necessary to contact the IT department if the breach requires their assistance, e.g. if you need help to remove possible malware and/or virus.

It’s important that the actual circumstances are continuously documented as this might be important information that’s crucial to the assessment of the risk for the data subject and a possible notification to the DPA (Data Protection Agency). If the actual circumstances aren’t continuously documented, important information can get lost.

If you’re in doubt about what to do, you’re always more than welcome to reach out to the compliance team.

Inform the compliance team about the breach

It’s the compliance team that’s responsible for handling and assessing personal data breaches at [insert organization’s name here]. You’re therefore required to inform the compliance team as quickly as possible if there’s a personal data breach, as the deadline for notifying the DPA is short.

You can do this by writing to [insert email address of contact person in the organization] or get in direct contact with an employee of the compliance team. If it’s a serious personal data breach, it’s especially important you make sure that the message is delivered to the right person as quickly as possible.

**5. The compliance team’s assessment of the breach**

**5.1 Notification of the DPA**

The compliance team need to initially assess whether the breach is to be reported to the DPA.

As a rule all personal data breaches must be reported to the DPA **within 72 hours**. It’s only if it’s *unlikely* that the personal data breach involves a risk for the rights and freedoms of natural persons that is doesn’t need to be reported.

**5.2 Notification of the data subjects**

If it’s *likely* that a personal data breach involves a high risks for the rights and freedoms of natural persons, [insert organization’s name here] must notify the data subjects about the breach.

5.2.1. High risk

There is no fixed definition of what characterises a high risk for the data subject, but the more serious consequences the breach is assessed to have, and the higher the likelihood is that these consequences materialise, the higher the risk to the data subjects is assessed to be. All possible consequences and negative effects, for the data subject, must be considered when it’s being assessed whether there’s a high risk for the data subject. In addition, a concrete risk assessment must be made to determine the specific consequences the data breach could have for the data subject. It’s important the assessment is reasonable and objective. Furthermore the compliance team needs to make sure that all necessary measures have been taken to limit/stop the breach.

If risk assessments have already been made (in regards to the data subject), it would make sense to have a look at these in this context, as they’ll typically show the risk for the data subject in connection to the system, process or processing activity involved in the mentioned breach.

5.2.2. The content of the assessment

The assessment must look into all relevant circumstances.

Below is a list of some of the factors that should always be included in the assessment:

The type of breach

It affects the assessment what type of breach it is.

The type of personal data

The type of personal data affects the assessment. The more confidential personal data it involves, the higher the consequence a breach assumedly has for the persons concerned.

Category of data subjects

The assessment must take into account the category of data subjects that’s affected by the breach. It can be aggravating if it concerns children or groups particularly at risk.

The extend of the breach

The risk assessment must take into account the amount of personal data and/or the amount of data subjects that is affected by the breach.

The time extend of the breach

The time extend of the breach may also influence the assessment. This is because the risk for the data subject may be higher if the data have been accessible over an extended period of time.

The possibility of identifying persons

The possibility of identification also influences the risk assessment. It will e.g. be more difficult to identify the concerned persons if the data, which the breach involve, are encrypted.

Consequences for the data subjects

The assessment must take into account what consequences the breach might have for the data subjects.

5.2.3. How to carry out the notification

The data subject must be informed without undue delay after the breach has been detected.

The notification must be given directly to the data subject, e.g. via letter, email or phone message. A press release is not sufficient.

5.2.4. Exemptions from the notification requirement

There is no notification requirement for the data subjects if:

* The data controller has implemented appropriate technical and organisational security measures, and these measures have been applied to the personal data that are affected by the personal data breach, mainly measures that make the personal data incomprehensible for anyone without authorised access, e.g. like encryption.

**Document Information**

|  |  |
| --- | --- |
| Document Version |  |
| Date of Issue for This Version |  |
| Responsible Person |  |
| Status |  |