|  |
| --- |
| **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].

|  |
| --- |
| The text boxes in the document contain focus points and good advice for you as a data controller or data processor. Please note that the text boxes should be removed from the final version of the specific policy or procedure. |

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.

**Procedure for handling personal data breach**

This procedure is designed as a checklist of the various steps that need to be taken in connection with a personal data breach.

When a personal data breach has been identified, you must:

**1. Get an overview**

Make sure to identify and describe what is currently possible. This will help you with the next steps in the process.

**2. Stop the accident**

If it is an ongoing personal data breach, it is very important to stop it to minimize any consequences for the data subject. At the same time, it is important that the actual circumstances are documented continuously, as important information may otherwise be lost.

**3. Assess whether the personal data breach should be reported to the relevant supervisory authority**

As a rule, all personal data breaches must be reported to the relevant supervisory authority within 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The assessment of whether there is a risk to the rights and freedoms of the data subject must be based on:

* The type of security breach, including whether there has been a loss of data, a breach of confidentiality or an integrity violation.
* The nature and extent of the information.
* The risk of the data subject(s) being identified.
* The consequences the breach may have for the data subjects.
* Whether the breach involves special data subjects (e.g. children or particularly vulnerable persons).
* The number of data subjects affected.

It is crucial that the assessment is objective and impartial - and furthermore, all considerations and decisions in the process must be documented, see point 5 below.

|  |
| --- |
| If you have already carried out risk assessments (in relation to the data subject) in your organization, it will be obvious to look at these in this context, as they will typically express the risk to the data subject in relation to a system, process, or processing activity. |

**4. Assess whether the data subject should be notified**

If a personal data breach is to be reported to the relevant supervisory authority, it must also be assessed whether the data subject should be notified of the data breach.

The data subject must be notified if the data breach is likely to result in a high risk to the rights and freedoms of the data subject. This gives the data subject the opportunity to take a number of precautions to mitigate any risks.

4.1. High risk

There is no fixed definition of what constitutes a high risk to the data subject, but the more serious the consequences of the data breach are assessed to be, and the more likely the consequence is to occur, the higher the risk to those affected must be assessed to be.

All possible consequences and negative effects, for the data subject, must be considered when assessing whether there is a high risk to the data subject.

4.2. Who, when and how should the notification be made?

The data controller is responsible for notifying the data subject.

The data subject must be notified without undue delay after the personal data breach has been identified.

The notification must be made directly to the data subject, e.g. by letter, e-mail, or text message. A press release is for example not sufficient.

|  |
| --- |
| If you already have a template for notifying the data subject, you can link to it here. |

4.3. Exceptions to the notification requirement

There is no requirement for notification if:

* The data controller has implemented appropriate technical and organizational security measures that have been applied to the personal data concerned by the data breach, e.g. if the data is protected by encryption.
* The high risk to the data subject is no longer real, e.g. in a case where there has been unauthorized access to personal data, but where it has been documented with certainty that no unauthorized persons have accessed the data.
* The notification requires a disproportionate effort. This may be the case where, in connection with a data breach, the information about the data subjects who should be notified has been lost. In this case, a public notice or a similar measure must be issued.

**5. Remember the internal documentation**

Regardless of whether it has been assessed that a personal data breach should be reported to the relevant supervisory authority or not, it must be documented, including the actual circumstances, key assessments in relation to the handling of the data breach, and actions taken.

|  |
| --- |
| **Information to [Insert relevant parties]**  In some organizations, it may be relevant to make an orientation/reporting when a personal data breach has been identified or reported. This could be, for example, to the immediate manager, the management, the group management, or the ministry. |

**6. Evaluation**

Any breach of personal data security should be followed up by an evaluation, where the following questions may be relevant:

* Is this the first time this type of breach of personal data security has occurred, or is it a recurrence?
* If this is the first time this type of breach of personal data security has been detected, it may be beneficial to follow up with extra awareness in the individual process/department or together with the individual employee.
* If it is a recurrence, the process should be reviewed to assess whether there should be further awareness measures or whether mitigating measures should be taken in the process.

The evaluation should also be documented.

**Document Information**

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