**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 for all companies. If this is the case, it will be clearly indicated in the text.

|  | Text boxes in the document contain focus points and good advice. Please note that the text boxes should be removed from the final version of the specific policy or procedure. |  |
| --- | --- | --- |

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

At the end 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: |  |
| --- | --- | --- |
|  | * You can add or remove sections, change the wording, and add your own logo and branding.
 |  |
|  | * Stay up-to-date with your templates. Data protection and information security regulations are evolving rapidly, so it's crucial to keep your templates current.
 |  |
|  | Should you have any inquiries concerning the templates, please feel free to contact us. |  |

### **Procedure for Handling Personal Data Breaches**

This procedure is designed as a checklist of the various steps to be taken in the event of a personal data breach.

| If the data breach concerns a customer's data (the data controller), the data breach must be reported to the data controller, **see point 7.** |
| --- |

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

**1. Get an Overview**

Ensure that you have identified and described what is possible at the present time. In this way, you are better prepared for the next steps in the process.

**2. Stop the Breach**

If there is an ongoing data breach, it is very important to stop this, so that any potential consequences for the data subject are minimized. At the same time, it is important to document the actual circumstances on an ongoing basis, as important information that is crucial for assessing the risk to the data subject and any potential notification to the relevant Data protection supervisory authority may otherwise be lost.

**3. Assess Whether the Personal Data Breach Must Be Reported to the relevant Data protection supervisory authority**

As a general rule, all personal data breaches must be reported to the relevant Data protection supervisory authority within 72 hours. Thus, it is only if it is unlikely that the personal data breach will pose a risk to the rights or freedoms of natural persons (the data subject) that a notification need not be made.

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

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

It is essential that the assessment is objective and factual – and in addition, all considerations and decisions in the process must be documented, see point 5 below.

**4. Assess Whether the Data Subject Must Be Notified**

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

Notification of the data subject must take place if the data breach is likely to result in a high risk to the rights or freedoms of the data subject. This gives the data subject the opportunity to take a number of measures to mitigate any potential risks.

4.1. High risk

There is no fixed definition of what is characterized as a high risk to the data subject, but the more serious the consequences of the data breach are assessed to be, and the greater the likelihood that the consequence will occur, the higher the risk to the data subject must be assessed.

All possible consequences and negative effects for the data subject must be taken into account when assessing whether there is a high risk for the data subject.

4.2. Who, when and how should the notification take place

It is the data controller who notifies the data subject.

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

The notification must be sent directly to the data subject, e.g. by letter, email or SMS. A press release, for example, is not sufficient.

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, which have been applied to the personal data in question that have been affected by the data breach, e.g. if the data is protected by encryption.
* the high risk to the data subject is no longer real, for example in the case where there has been an opportunity for 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 if, in connection with a data breach, the information about the data subjects who should be notified has been lost. In this case, a public announcement or a similar measure must be made.

**5. Remember the Internal Documentation**

Regardless of whether it has been assessed that a personal data breach must be reported to the relevant Data protection supervisory authority, it must be documented. The actual circumstances, significant assessments in relation to the handling of the data breach, and the measures taken must therefore be documented.

**6. Evaluate**

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

* Is this the first time this type of personal data breach has occurred or is it a repetition?
* If this is the first time this type of personal data breach has been identified, it may be advisable to follow up with additional awareness in the individual process/department or with the individual employee.
* If this is a repetition, a closer look should be taken at the process to assess whether there should be additional awareness measures, or whether mitigating measures should be taken in the process.
* The evaluation should also be documented.

| **7. Notification to the Data Controller** If a personal data breach involves customer data, the data controller must be notified as soon as possible. The notification and subsequent communication must also be documented. |
| --- |

**Document information**

| Document version |  |
| --- | --- |
| Date of Issue for this version |  |
| Responsible Person |  |
| Status |  |