|  |
| --- |
|  **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.

|  |
| --- |
| 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.  |

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.

**Procedure for Handling of Data Processing Agreements**

**1. Purpose**

This procedure describes:

* [Insert organization name]'s procedure for entering into data processing agreements with [Insert organization name]'s data processors (section 2).
* [Insert organization name]'s procedure for controlling data processing agreements that have been entered into with [Insert organization name]'s data processors (section 3).
* [Insert organization name]'s procedure for entering into data processing agreements with customers (section 4).

**2. Entering into Data Processing Agreements**

Before using a new supplier, the compliance officer assesses whether the supplier is a data processor for [Insert organization name] because a data processing agreement must then be entered into.

The data processing agreement must be drawn up in accordance with Article 28(3) of the General Data Protection Regulation. The compliance officer assesses the requirements to be imposed on the data processor in question; including the technical and organizational security measures that the data processor must have implemented.

Only [INSERT NAME/POSITION] can enter into binding data processing agreements.

**3. Data Processor audits**

The compliance officer assesses:

1. How often it is necessary to audit each of [Insert organization name]'s data processors.
2. What type of audit should be carried out for each of [Insert organization name]'s data processors, and in this connection, sets up a task to audit the respective supplier on [Insert organization name]'s site in Wired Relations.

The assessment of how often a data processor must be audit and which audit must be carried out shall be based on [insert relevant assessment, for example: the Danish Data Protection Agency's guidelines on audit of data processors].

However, data processors that are sub-processors of [Insert organization name]'s customers must be audited at least once a year.

**4. Entering into Data Processing Agreements with Customers**

Only [INSERT NAME/POSITION] can enter into binding data processing agreements with customers.

When entering into a data processing agreement with a customer, it must be ensured that the data processing agreement is in accordance with data protection legislation and that the agreement is in accordance with [Insert organization name]'s information security policy and the policies, guidelines, and procedures that flow from it.

If a customer requires that [Insert organization name] has implemented specific security measures, it must be investigated whether the security measure in question has been implemented before entering into the data processing agreement in question.

It must also be investigated whether the security measure in question has been implemented at [Insert organization name]'s sub-processors.

4.1 Use of Sub-Processors

When using a sub-processor, it must be ensured that a data processing agreement is entered into with the sub-processor.

The data processing agreement must reflect that the security level agreed with the customer is also ensured by the sub-processor. It must also be ensured that the sub-processor acts according to the same instructions.

[Insert organization name] only uses sub-processors that are approved by customers who have entered into a data processing agreement with [Insert organization name].

The data processing agreements stipulate, as a starting point, that [Insert organization name] has general approval to use sub-processors on the condition that the customers in question are notified.

Therefore, when adding new sub-processors, customers must be notified in accordance with the data processing agreements. The notification must be made in a timely manner so that customers have the opportunity to object and/or withdraw personal data.

If a data processing agreement is entered into with a requirement for specific approval of sub-processors, specific approval must be obtained from the customers in question before the sub-processor in question is used.

The addition of new sub-processors must also be carried out in accordance with [Insert organization name]'s guidelines for the commissioning of new suppliers.

**5. Follow-up**

This procedure is evaluated annually.

### **Document Information**

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