**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 Data Processor Agreements**

**1. Purpose**

This procedure describes: *[insert company's name]*'s procedure for entering into data processor agreements with *[insert company's name]*'s data processors (section 2)

*[insert company's name]*'s procedure for controlling data processor agreements entered into with *[insert company's name]*'s data processors (section 3).

| *[Insert company's name]*'s procedure for entering into data processor agreements with customers (section 4) |
| --- |

**2. Entering into Data Processor Agreements**

Prior to the use of a new supplier, the compliance officer shall assess whether the supplier in question is a data processor for *[insert company's name]*, as in that case a data processor agreement must be entered into.

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

Only *[insert name/position]* may enter into binding data processor agreements.

**3. Data Processor Audits**

The compliance officer shall assess:

1. how often it is necessary to audit each of *[insert company's name]*'s data processors.
2. What type of audit should be carried out for each of *[insert company's name]*'s data processors, and in this connection create a task to audit the respective supplier on *[insert company's name]*'s site in Wired Relations.

The assessment of how often a data processor should be audited, and what type of audit should be carried out, must be based on guidelines on auditing data processors (in Denmark the Danish Data Protection Agency's guidelines on auditing data processors)

Data processors who are sub-data processors of *[insert company's name]*'s customers must, however, be audited at least once a year.

| **4. Entering into Data Processor Agreements with Customers**  Only *[insert name/position]* may enter into binding data processor agreements with customers.  In connection with the conclusion of a data processor agreement with a customer, it must be ensured that the data processor agreement complies with the data protection rules, and that the agreement is in accordance with *[insert company's name]*'s information security policy and the policies, guidelines and procedures that derive therefrom.  In the event that a customer requires *[insert company's name]* to have implemented specific security measures, it must be investigated whether the security measure in question has been implemented before the conclusion of the data processor agreement in question.  It must also be investigated whether the security measure in question has been implemented at *[insert company's name]*'s sub-data processors.  4.1 Use of sub-data processors  When using a sub-data processor, it must be ensured that a data processor agreement is entered into with the sub-data processor. The data processor agreement must reflect that the level of security agreed with the customer is also ensured by the sub-data processor. It must also be ensured that the sub-data processor acts in accordance with the same instructions.  *[insert company's name]* only uses sub-data processors who are approved by customers who have entered into a data processor agreement with *[insert company's name]*.  The data processor agreements generally stipulate that *[insert company's name]* has general approval to use sub-data processors provided that notification is given to the customers in question.  When adding new sub-data processors, customers must therefore be notified in accordance with the data processor agreements. Notification must be made in good time so that customers have the opportunity to object and/or withdraw their personal data.  In the event that a data processor agreement is entered into with a requirement for specific approval of sub-data processors, specific approval must be obtained from the customers in question before the sub-data processor in question is used.  The addition of new sub-data processors must also be in accordance with *[insert company's 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 |  |