**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. |  |

**Deletion Policy for *[insert company’s name]***

**1. Purpose**

The purpose of this deletion policy is to establish guidelines for when personal data should be deleted, ensuring that *[insert company's name]* does not retain personal data for longer than necessary.

**2. Scope**

This policy applies to [Company Name], including all employees, whether full-time, part-time, or freelance consultants.

**3. Retention and Deletion**

3.1 General Deletion

Personal data processed by *[insert company's name]* must be accurate, and steps must be taken to promptly delete or correct inaccurate or faulty personal data.

The permissible retention period for different types of personal data must always be assessed and determined based on a specific assessment of how long there is a legitimate need to retain the data.

Upon expiration of the retention period, personal data must be deleted or alternatively anonymized.

If a data subject submits a request for deletion, the request must be processed, and the data subject must be informed of the outcome of the processing within one month, in accordance with Article 12(3) of the GDPR.

3.2 Specific Requirements for Retention Period

As a general rule, personal data may not be stored for a longer period than is necessary to fulfill the purpose(s) for which the data is processed.

| However, there may be specific legislation that imposes specific requirements on the retention period, and it is therefore important to identify which specific legislation applies to your company. For example, the Danish accounting law requires retention for the current financial year plus five years. There are also statements from other authoritative sources that can help determine retention periods. For example, the Danish Consumer Ombudsman's guidelines on spam state that information that a person has consented to receive marketing in accordance with the marketing law must be stored for 2 years from the last contact with the person in order to document the consent. |
| --- |

The retention period may be extended in certain situations based on commercial and legal needs to document cases, processes, and decisions, etc.

For example, it may be necessary to retain personal data as long as it may be relevant for *[insert company's name]* to make a claim or protect itself against claims based on documents, etc. containing personal data.

If there is a need to extend a retention period, this should always be clarified with the data protection officer at *[insert company's name]*.

3.3 Anonymization

If personal data is anonymized, the data loses its character as personal data, and the data is therefore no longer subject to data protection legislation. Anonymized data is therefore not subject to the requirement for deletion.

Anonymization can be an alternative to deletion.

3.4 Data Processor Agreements

**Note:** If *[insert company's name]* acts as a data processor for personal data, a specific section addressing this role should be included here.

**Note:** If not covered in other policies, this section should outline the requirements for deleting personal data when working with suppliers and data processors. This includes procedures for returning personal data from these entities.

### **4. Deletion Procedure**

To ensure that a decision has been made on the procedures to be followed when deleting personal data from individual processing systems, a deletion procedure must be completed for each system. A deletion procedure for a given system in which personal data is processed should be based on a flow from the time the deletion deadline occurs until the deletion is completed and confirmed in the system.

As a general rule, the system user will identify the deletion deadlines, and the system owner will be responsible for initiating and maintaining the deletion procedure for the individual system.

| Wired Relations has developed a deletion procedure template that can be used if desired to describe the deletion procedure for the company's systems. |
| --- |

### **5. Follow-up**

We continuously monitor compliance with the deletion policy, including ensuring that deletion and any return from suppliers actually takes place in accordance with the policy.

We also regularly review the deletion policy to assess whether changes are needed, for example, due to changes in legislation or other internal policies that affect this policy.

**Document information**

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