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

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.

Here are some links to additional resources that you may find helpful:

* The Danish Data Protection Agency: [https://datatilsynet.dk/](https://datatilsynet.dk/" \t "_blank)
* The Danish Centre for Cybersecurity:  [Center for Cybersikkerhed (cfcs.dk)](https://www.cfcs.dk/da/)

**Deletion Policy for [Insert Organization Name]**

**Purpose**

In order to comply with applicable legislation, personal data should not be stored for a longer period than necessary to fulfill the purpose(s) for which the personal data are processed.

The purpose of this deletion policy is to establish guidelines for when personal data should be deleted, so that it is ensured that [Insert Organization Name] does not store personal data for longer than necessary.

**Scope**

This deletion policy applies to [Insert Organization Name], including all employees, whether employed full-time, part-time, freelance or as consultants.

**Storage and Deletion**

General Information on Deletion

Personal data processed by [Insert Organization Name] as data controller must be accurate and steps must be taken to promptly rectify or erase inaccurate or incomplete personal data.

The permitted storage period for different types of personal data must always be assessed and determined on the basis of a specific assessment of how long there is a legitimate need to store the data.

At the end of the storage period, the personal data must be deleted or anonymized.

If a data subject requests deletion, the request must be processed and the data subject must be informed of the outcome of the processing within one month, cf. GDPR Article 12, paragraph 3.

**Special Requirements for Storage Period**

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

However, there may be specific legislation that imposes special requirements for the storage period, and it is therefore important to identify which specific legislation applies to your organization. For example, the Danish Accounting Act requires storage for the current financial year plus five years.

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

For example, it may be necessary to store personal data for as long as it may be relevant to [Insert Organization Name]'s ability to assert claims or protect itself against claims based on documents, etc., containing personal data.

If there is a need to extend a storage period, this should always be clarified with the data protection officer at [Insert Organization Name].

Anonymisation

If personal data is anonymized, the data loses its character of being personally identifiable, and the data is therefore no longer covered by data protection legislation. Anonymized data is therefore not subject to the deletion requirement.

Anonymisation can be an alternative to deletion.

Data Processing Agreements

If [Insert Organization Name] processes personal data as a data processor, a section on this must be written below.

If not stated in other policies, requirements for deletion to suppliers and data processors must also be stated in this section. This includes whether personal data must be returned from a data processor or supplier.

**Deletion Procedure**

In order to ensure that it has been determined which procedures must be followed when personal data must be deleted from the individual processing system, a deletion procedure must be completed for each system. A deletion procedure for a given system in which personal data are processed should be based on a flow from the time the deletion period expires until the deletion has been carried out and confirmed in the system.

As a general rule, it will be the user of the system who identifies the deletion periods, and the system owner who is responsible for implementing and maintaining the deletion procedure for the individual system.

See template for deletion procedure.

**Follow up**

We continuously monitor compliance with the deletion policy, including 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 there is a need for changes, for example as a result of changes in legislation or other internal policies that affect this policy.

### **Document Information**

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