|  |
| --- |
| **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.

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/>
* The Danish Centre for Cybersecurity:  [Center for Cybersikkerhed (cfcs.dk)](https://www.cfcs.dk/da/)

**Introduction**

In order to ensure that procedures are in place for the deletion of personal data from a processing system, a deletion procedure must be completed for each system.

It is recommended that the deletion of personal data be considered from the outset of processing. This will allow the processing to be designed in a way that any different deletion periods can be met in an appropriate and possibly automated manner.

A deletion period is defined based on the purpose of the processing of the personal data in question.

[Insert organization name] Data Protection Officer can be contacted if you have any questions about the procedure.

|  |  |
| --- | --- |
| **Deletion Procedure Template for:** *[Insert System Name]* | |
| What personal data is processed in the system?  **Note:** You can find this information in the inventory, or by checking the system details in WR. | *Example: Name, address, and job applications* |
| What is the deletion period for each type of personal data in the system? | *Example: Deletion period for job applications is 6 months*  *Deletion period for name and phone number is 12 months* |
| How is the data deleted (manually or automatically - and explain how it is done)? | *Describe here* |
| Which specific data fields will be affected by the deletion, and in what way?  This could involve, for example, a customer at a company having their entire data sheet deleted from the system, or only the personally information being deleted or anonymized. | *Describe here* |
| Who is responsible for carrying out the deletion? | *Describe here* |
| How is it followed up on whether the deletion has been carried out? And who is responsible for the follow-up? | *Describe here* |
| How is it documented that the deletion has been carried out? | *Describe here* |
| What follow-up procedure for deletion has been implemented? | *Example: Review of technical logs from deletion runs, i.e., automated extraction of data that should have been deleted according to the deletion period.* |
| How is the system continuously checked for personal data that has reached its deletion period? | *Describe here* |
| How is it ensured that the data is also deleted from backups, so that deleted personal data is not reloaded when the backup is restored? | *Describe here* |
| If it is not technically possible to delete individual data from a backup, it must be ensured that the personal data that has been deleted from the live system is deleted if the backup is restored. How is this done?  **Note:** A log of this can be kept but be aware that it should not contain personal data, but instead should indicate a given row in a table that was deleted at a given time. | *Describe here* |

### **Document Information**

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