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

**Policy for the processing of personal data**

**1. Purpose**

This policy describes the basic concepts, principles and guidelines that are important for you as an employee to know and work from when you process personal data.

**2. Introduction**

The data protection legislation, including the General Data Protection Regulation (GDPR), sets out a number of rules for how a company may process personal data.

The company must establish guidelines for, and instruct you on, how you, as an employee, help to ensure that the company complies with the legislation.

As an employee of [insert organization’s name here], you are required to act in accordance with this policy and follow the guidelines below.

**3. Important concepts**

The data protection legislation applies to a company's *processing* of *personal data*. It is therefore important that you know what it means to process personal data.

*Personal data* is information that can be used to identify a specific person, or information about a person who has already been identified.

*Processing* refers to anything you can do with personal data. It is, for example, considered to be processing when you collect, register, store or pass on personal data.

Both the concept of personal data and the concept of processing must be understood very broadly.

**4. Categories of personal data**

A distinction is made between non-sensitive and sensitive personal data. It is important that you know whether you are processing non-sensitive or sensitive personal data, because different rules apply to the two categories of personal data. In addition, you should know that the social security number and information about criminal offences are separately regulated, and that special rules therefore apply when/if you process these.

Non-sensitive personal data

Non-sensitive personal data is all personal data that cannot be categorised as sensitive. Examples of non-sensitive personal data are: name, address, salary information, shoe size and hair colour.

Sensitive personal data

Sensitive personal data is exhaustively listed in the GDPR article 9, and is information about:

* race or ethnic origin
* political, religious or philosophical beliefs
* trade union affiliation
* genetic data
* biometric data regarding unique identification
* health information
* sexual relationships or sexual orientation.

As a rule, you will not process sensitive personal data, social security numbers or information about criminal offences when you work at [insert organization’s name here].

If you need to process these types of personal data, you are obliged to clarify whether you are authorised to carry out the processing. This must be done in collaboration with the compliance team.

**5. Important principles**

The data protection law sets out a number of principles that you must follow every time you process personal data.

This section highlights the principles that are particularly important for you to know and actively use when processing personal data.

The principles ensures that the processing of personal data is always limited to what is necessary to ensure that the processing takes place in a secure manner for a valid and legitimate purpose.

**5.1. Legality**

Personal data must be processed lawfully. This means that you must have a legal basis to carry out a processing. If you are in doubt as to whether you have a legal basis to process personal data, you are obliged to clarify this with the compliance team.

**5.2 Transparency**

Personal data must be processed transparently. This means that the data subject must know which personal data is being processed about them.

As a rule, the data subject will be informed about this in the company's privacy policy.

The data subject also has the right to know how you process the personal data of the person concerned. It is therefore important that you always process personal data in a way that can withstand coming to the knowledge of the data subject.

If you carry out processing where you are in doubt as to whether the data subject has been informed about the processing, you are obliged to clarify this with the compliance team.

It is also important that you involve the compliance team if you intend to start a new type of processing of personal data. This is because the company is obliged to inform the data subject about the processing and to keep a record of the processing carried out in the company.

**5.3. Purpose**

The personal data may only be collected for explicitly stated and legitimate purposes. This means that you must always be able to explain the purpose for which you have collected personal data. You must also be able to explain the purpose for which you carry out further processing of information that you already have.

If you are in doubt as to whether the processing you want to carry out has a legitimate purpose, you are obliged to clarify this with the compliance team.

**5.4. Minimisation**

The processing of personal data must be sufficient, relevant and limited to what is necessary. This means that you must not process personal data that goes beyond what is necessary to fulfil the purpose of the processing.

You can distinguish between personal data that is 'nice to have' and personal data that is 'need to have'. You may only process information that is 'need to have'.

You may also only store the personal data for as long as necessary. This means that you must delete personal data when you no longer have a purpose for storing it.

You must always be able to explain why you are in possession of personal data.

**5.5. Integrity and Confidentiality**

You must process personal data in a secure manner. This means that you must take care of the personal data that you process. You do this primarily by following the guidelines in this policy as well as by following the company's other guidelines, policies and procedures.

If you believe that any additional measures should be taken in order for a processing to be safe, you are obliged to take these.

If you discover that some of the personal data you are processing is incorrect, you are also obliged to correct or delete it.

**6. Follow-up**

This policy is evaluated once a year by the compliance team.

The purpose of this information security policy is to establish the framework for the work with information security within [insert organization’s name here]. The policy creates the foundation upon which the work with information security is established.

The purpose of the policy is also to create a common consensus of what information security is as a whole and define both goals and the division of responsibilities for the work with information security within [insert organization’s name here].

### **Document Information**

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