**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. |  |

**Personal Data Processing Policy**

**1. Purpose**

| The purpose of this policy is to provide company employees with a comprehensive overview of data protection, including the rights and obligations arising from the General Data Protection Regulation (GDPR). More operational aspects, such as the specific handling of data breaches and subject access requests, may be detailed in separate procedures.  Wired Relations also offers templates for these procedures. |
| --- |

This policy outlines the fundamental concepts, principles, and guidelines that are essential for employees to understand and follow when processing personal data.

**2. Introduction**

Data protection legislation, including the GDPR, establishes a set of rules governing how companies may process personal data. The company must define guidelines and instruct employees on how to ensure compliance with the legislation.

As an employee of *[insert company's name]*, you are obligated to adhere to this policy.

**3. Key Terms**

Data protection legislation applies to a company's processing of personal data. It is therefore important to understand the meaning of "processing" personal data.

Personal data refers to any information that can be used to identify a specific individual or information about an individual who has already been identified.

Processing encompasses any action performed on personal data, such as collection, recording, storage, or disclosure.

Both "personal data" and "processing" should be interpreted broadly.

**4. Categories of Personal Data**

A distinction is made between general and sensitive personal data. It is important to know whether you are processing general or sensitive personal data, as different rules apply to each category. Additionally, you should be aware that the civil registration number (CPR number) and information about criminal convictions are subject to specific regulations.

General personal data refers to all personal data that cannot be categorized as sensitive. Examples include name, address, salary information, shoe size, and hair color.

Sensitive data is exhaustively listed in the GDPR and includes information on:

* Race or ethnic origin
* Political, religious, or philosophical beliefs
* Trade union membership
* Genetic data
* Biometric data for the purpose of uniquely identifying a natural person
* Health data
* Sexual orientation

| The determining factor for whether information should be considered confidential is an assessment of whether, according to the general view in society, the information should be kept confidential.  Sensitive personal data will undoubtedly be confidential. Conversely, confidential information is not always sensitive.  Non-sensitive personal data can be confidential in certain situations. The Data Protection Agency cites examples such as income and wealth, employment, education, and employment-related matters, and internal family matters. Additionally, a civil registration number (CPR number) is also considered confidential personal data. |
| --- |

If you are unsure whether you are permitted to process specific personal data, please contact *[insert relevant contact point, e.g., DPO]*.

### **5. Key Principles**

Data protection legislation sets out a number of principles that you must follow whenever you process personal data.

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

These principles ensure that the processing of personal data is always limited to what is necessary to ensure that processing is carried out securely for a legitimate purpose.

5.1 Lawfulness

Personal data must be processed lawfully. This means that you must have a legal basis for processing. If you are unsure whether you have a legal basis for processing personal data, you are obligated to clarify this with *[insert relevant contact point, e.g., DPO*].

5.2 Fairness and Transparency

Personal data must be processed fairly and transparently. This means that the data subject must be informed about the personal data being processed. This information is typically provided in the company's privacy policy.

The data subject also has the right to know how their personal data is being processed. It is therefore important to always process personal data in a manner that can be disclosed to the data subject.

If you are unsure whether the data subject has been informed about the processing, you are obligated to clarify this with *[insert relevant contact point, e.g., DPO]*.

It is also important to involve *[insert relevant contact point, e.g., DPO]* if you are considering starting a new type of personal data processing. This is because the company is obligated to inform the data subject about the processing and to maintain a record of the processing activities.

5.3 Purpose Limitation

Personal data may only be collected for specified, explicit, and legitimate purposes. This means that you must always be able to justify the purpose for which you have collected the data. You must also be able to justify the purpose for any further processing of the data.

If you are unsure whether the processing you intend to carry out serves a legitimate purpose, you are obligated to clarify this with *[insert relevant contact point, e.g., DPO].*

5.4 Data Minimization

The processing of personal data must be adequate, relevant, and limited to what is necessary. This means that you must not process personal data that goes beyond what is necessary to fulfill 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 should only process data that is "need to have."

You should also only retain personal data for as long as necessary. This means that you must delete personal data when you no longer have a purpose for retaining it.

You must always be able to justify why you possess personal data.

5.5 Accuracy

You must take every reasonable step to ensure that the personal data you process is accurate and, where necessary, kept up to date.

If you become aware of inaccurate personal data, you are obligated to rectify it.

**6. Storage of Physical Material Containing Personal Data**

In principle, the same rules apply to the secure storage of personal data, whether it is physical or digital material containing personal data. Therefore, only trusted individuals with a legitimate need should have access to physical documents containing personal data.

| If your company has established guidelines for storing physical material containing personal data, these can be described below.  Examples:   * Physical material containing personal data should be stored locked when not in use. * Physical material containing personal data should only be accessible to trusted employees who have a legitimate need to access the material. * Physical material should be destroyed in a secure manner when the purpose of storage ceases (e.g., by shredding or burning). |
| --- |

**7. Data Protection Officer**

| If your company is obligated to appoint a Data Protection Officer, or if you have voluntarily appointed one, you can describe the function in more detail in this section.  Example: The Data Protection Officer at *[insert company's name]* is *[insert name of Data Protection Officer].* The primary task of the Data Protection Officer is to advise the company on all data protection law matters, and it is therefore important that the Data Protection Officer is involved in a timely manner.  You should always consult with the Data Protection Officer if you are considering purchasing a new IT system, entering into an agreement with a new supplier, initiating a new process involving the processing of personal data, or if there has been a personal data breach. |
| --- |

**8. Follow-up**

This policy is evaluated once a year by the company's internal compliance team.

**Document information**

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