|  |
| --- |
| **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.

|  |
| --- |
| Text boxes in the document contain focus points and good advice for you as a data controller or data processor. 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 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.

**Overall Data Protection Policy for [Organization Name]**

|  |
| --- |
| The purpose of this policy is to provide an overview of data protection for employees of [Organization Name], 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 access requests, can be described in separate procedures. Wired Relations' framework includes templates for this purpose. |

Everyone has the right to the protection of their personal data, and anyone who processes personal data about others (except in a private context) is obliged to observe these rights and to protect personal data.

**Why is it important to know about data protection?**

It is essential that all employees who process personal data as part of their work are equipped to process the data in the right way. Lack of knowledge in this area leads to an increased risk of data breaches, and thus also a greater risk for the data subject.

**What is personal data?**

Personal data is any information that can be attributed to a specific person, even if the person can only be identified if the information is combined with other information.

The General Data Protection Regulation (GDPR) divides personal data into three types:

* Ordinary personal data
* Sensitive personal data
* Data on criminal offenses (convictions and offenses or related security measures)

**When is personal data processed?**

The concept of "processing" of personal data must be understood very broadly, and in practice it means that any handling of personal data about others is processing. This can include, for example, collection, registration, organization, systematization, storage, adaptation or modification, as well as retrieval, search, use, disclosure by transmission, dissemination or any other form of disclosure, matching or combination, restriction, deletion or destruction.

**When is it permitted to process personal data?**

When processing personal data, it is a requirement that there is a legal basis for doing so, and this depends on the type of personal data in question.

|  |
| --- |
| If you want to get a little more text for this section, you can choose to insert completely general examples:   * **Ordinary personal data -** the legal basis must be found in Article 6 of the GDPR. * **Sensitive personal data -** the legal basis must be found in Article 9 of the GDPR. * **Criminal offenses -** the legal basis must be found in Article 10 of the GDPR.   You can also choose to give concrete examples from your own everyday life, for example in relation to HR administration or customer service. |

**Basic principles**

Article 5 of the GDPR sets out a number of principles that are important to know when processing personal data. In addition to there being a valid legal basis for processing, these basic principles must always be met. As an employee of [Organization Name], it is important that you are aware of these principles and that you have a general understanding of what they cover.

* Purpose limitation
* Data minimization
* Lawfulness, fairness and transparency
* Accuracy
* Integrity and confidentiality
* Storage limitation

In addition to the basic principles, it is crucial that an organization demonstrates accountability and can document that the organization complies with the rules of the GDPR, including the basic principles.

|  |
| --- |
| If you want a more detailed description of the principles, you can start with the following.The principle of purpose limitationWhen an organization collects personal data about customers or employees, it may only collect personal data for clearly defined and specific purposes. The purpose must be limited.Personal data may be collected and processed for multiple purposes if there is a legal basis for this, for example by obtaining consent. The first time an organization collects personal data for a specific purpose, the data subject (the person about whom personal data is collected) must be informed of this.When personal data is collected for a specific purpose, this also means that the personal data may not be further processed for other purposes. For example, personal data may not be resold if the customer has not been informed of this specific purpose at the time of collection.It may be permissible to further process the collected personal data for legitimate or business purposes (as long as this is compatible with the original purpose). For example, it follows from a trade with a customer that the purchase and transaction must be documented and booked. In this case, of course, you do not need to ask a data subject for permission to book the invoice or store a copy of the contract.The principle of data minimizationOnly the personal data necessary to solve the task at hand (the purpose of processing the personal data) should be collected.For example, it is of course necessary to have the customer's address if a package is to be delivered - but here, for example, it will not be necessary to collect information about marital status.You should only collect relevant personal data for the relevant purpose.The principle of lawfulness, fairness and transparencyAny processing of personal data must be lawful. An organization must have a legal basis for processing personal data, for example by obtaining consent from the customer.Any processing of personal data must be fair. It is fair to process personal data securely and based on best practice (e.g. available technological solutions, management standards, industry codes of conduct, etc.).An organization must process personal data in a transparent manner and be able to inform data subjects about it. Clear and easy-to-understand language must be used.The information must be clear and understandable to the target audience. Avoid using legal language.The principle of accuracyAn organization must ensure that the personal data processed is accurate.This means that the personal data must be kept up to date. It may also mean that the organization has some control measures in place to ensure that the personal data is always correct.The principle of integrity and confidentialityIntegrity An organization must ensure the integrity of personal data. This means that the reliability and correctness of the personal data must be ensured over time.Confidentiality An organization must ensure that personal data is processed with appropriate confidentiality. Unauthorized persons must not have access to personal data.Unauthorized persons can be hackers and thieves, but it can also be ordinary employees in the organization who have no work-related reason to access specific personal data.Adequate security In order to ensure the integrity and confidentiality of personal data, the organization must have implemented adequate and appropriate security. "Adequate security" depends on the organization's situation and is assessed on a risk-based approach.An adequate level of security may vary internally within an organization between the different processing of personal data (purposes). You can assess whether you have adequate security by carrying out a risk assessment of the individual processing of personal data. And based on a risk assessment, it can be assessed whether there is a need for additional technical or organizational measures, such as those that protect against unauthorized access to or use of personal data, including accidental loss, destruction or damage to personal data.The principle of storage limitationAn organization should only store personal data for as long as is necessary to complete a task (as long as there is a legitimate purpose for doing so). When it is no longer necessary to store personal data, the data should be deleted.Some systems cannot handle the deletion of personal data. In these cases, the personal data can instead be anonymized so that it is no longer possible to identify a natural person from the data. In this case, this will no longer be personal data - but just data.Personal data should never be stored or processed because it is the easiest solution or because it is "nice-to-have" for possible later use. In these situations, the personal data should be deleted.See more under "deletion policy" and "deletion procedure". |

**General security requirements for the processing of personal data**

The General Data Protection Regulation (GDPR) does not set any specific security requirements for the protection of personal data. Instead, it states that the data controller (or data processor) must implement appropriate security measures based on a specific risk assessment.

A security measure is, for example, the development of written policies and guidelines on how to process personal data.

In addition to this general data protection policy, we at [Organization Name] have developed various guidelines, all of which are aimed at ensuring better data protection and reducing the risk of data breaches. These can be found *[Insert link to the location where you store the developed guidelines].*

|  |
| --- |
| A distinction is made between technical and organizational security measures. Technical security measures can include antivirus programs, encryption, logging, pseudonymization, etc., and organizational security measures relate to the training and awareness of the organization's employees, as well as the establishment of guidelines and policies for the processing of personal data. |

**How personal data is processed via email**

Most of our communication takes place via email, and much of the personal data we process comes in via email. The email system is not a journaling system, and to ensure that personal data that should have been deleted or journalized long ago is not processed and stored, it is important to review the email system (inbox, subfolders, sent mail, and deleted mail).

|  |
| --- |
| There is no one-size-fits-all approach for email data handling guidelines. The best approach for your organization will depend on a number of factors, such as the size of your organization, the type of personal data you collect and process, and your risk tolerance.  However, there are some general guidelines that you can follow to ensure that personal data is processed in compliance with the GDPR when using email.  **EXAMPLE**  *Ordinary personal data*  Ordinary personal data can be sent and received via email.  Emails containing ordinary personal data can be stored in the email system as long as there is a legitimate purpose for doing so and as long as it is necessary for the task at hand. After this, the information must be deleted or archived if there is an obligation to store the information for a longer period of time, e.g. accounting documents.  *Sensitive and confidential personal data*  Emails with sensitive and/or confidential personal data must always be sent via a secure communication method, [insert the secure communication methods used by your organization].  In cases where you need to receive an email with sensitive and/or confidential personal data, you should refer the sender to send the information in a secure manner.  Sensitive and confidential personal data must be deleted from the email system within 30 days of receipt/dispatch. If there is an obligation to store the information for a longer period of time, the information must be archived (this may be the case for documentation of a course of illness that requires reimbursement - in this case, the information must be archived in the employee's personnel file). Remember to review both inbox, sent mail, and deleted mail.  Emails with sensitive and/or confidential personal data should be handled promptly. |

**Storage of physical material containing personal data**

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

|  |
| --- |
| If your organization has established guidelines for the storage of physical material containing personal data, it can be beneficial to describe them below.  Examples:   * Physical material containing personal data must be kept locked when not in use. * Physical material containing personal data must only be accessible to trusted employees who have a legitimate need to access the material. * Physical material must be destroyed in a secure manner when the purpose of storage ceases (describe how if applicable). |

**Data Protection Officer**

|  |
| --- |
| If your organization is obligated to appoint a Data Protection Officer (DPO), or if you have voluntarily appointed a DPO, you can describe the role in more detail under this section.  Example:  The Data Protection Officer at [Organization Name] is [DPO Name]. The DPO's primary role is to advise the organization on all data protection matters, and it is therefore important that the DPO is involved early on.  For example, you should always consult with the DPO if you are purchasing a new IT system, entering into an agreement with a new vendor, considering implementing a new process that involves the processing of personal data, or if there has been a data breach. |

### 

### **Document Information**

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