**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. |  |

### **Procedure for Handling Data Subject Access Requests (DSAR)**

This procedure is designed as a checklist of the various steps that must be remembered each time a request for access is to be answered.

**1. Receipt of a Request for Access**

When you receive a request for access, contact *[insert company's name]*, who is responsible for assessing and responding to requests for access in *[insert company's name]*.

A request for access must be answered as soon as possible, and at the latest one month after the request is made.

**2. Clarification**

Initially, it must be assessed whether the request can be answered in its current form, or whether it is relevant to investigate whether the request needs to be clarified, for example if the person wishes access to a specific area or a specific case.

Please note that you cannot refuse to answer a request for access in the event that the data subject does not wish to specify the request.

**3. Ensuring the Identity of the Data Subject**

When a person contacts and requests access to the personal data being processed about them, it must first be established that the person making the request is also the person they claim to be. In this way, it is ensured that there is no unintentional disclosure of personal data to unauthorized persons.

If the data subject is represented by others, it may be relevant to request a power of attorney.

Once the identity of the data subject has been established, and clarification of the request has been made, a receipt is sent to the data subject acknowledging receipt of the request.

**4. Identify and Collect the Personal Data Being Processed About the Person**

*[Insert relevant person in the company]* is responsible for identifying and collecting the personal data being processed about the person.

**5. Review the Material**

Once the relevant material has been identified and sent to *[insert relevant person in the company]*, the material must be reviewed.

If documents, etc., contain personal data about persons other than the data subject in question, this must be redacted or otherwise removed from the documents.

**6. Prepare a Response to the Data Subject**

Once the material has been reviewed, a response must be prepared for the data subject.

In addition to providing the data subject with a copy of the personal data being processed about them, the response must also contain information about:

* The purpose of the processing of personal data
* The categories of personal data
* The recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular if recipients are located in third countries or are international organizations.

In addition, the following must also be disclosed:

* If you transfer personal data to unsafe third countries or international organizations, and appropriate safeguards for data protection have been established, you must inform the data subject of these safeguards.
* If possible, you must also inform the data subject of the period for which you store the personal data or, if that is not possible, the criteria used to determine that period.
* Furthermore, you must inform the data subject that they have the right to request rectification, erasure or restriction of processing, that the data subject has the right to object to processing in specific situations, and that the data subject has the right to lodge a complaint with a supervisory authority (in Denmark the Danish Data Protection Agency).
* You must also inform the data subject of where the personal data originated. However, this only applies if the personal data in question has been collected from sources other than the data subject themselves.
* In the event that you use automated decision-making, including profiling, you must inform the data subject that they are subject to such processing, as well as the logic of the automated decisions. This includes, among other things, a description of the considerations underlying the processing and how the "system" arrives at the decisions.

In practice, a response is prepared with the above points, and a copy of the personal data (documents, reports, surveillance images, etc.) is attached.

**7. Send the Response to the Data Subject**

If the response to a request for access contains sensitive personal data, the response must be sent securely, for example (in Denmark via e-boks). If the response does not contain any sensitive personal data, it can be sent by email.

| **Specifically regarding our role as a data processor** If our customers (the data controller) need assistance in responding to a request for access, this is typically done through our normal support. |
| --- |

**Appendix 1 – Persons Responsible for Collecting Material**

| Here, you can advantageously list the systems in which you process personal data. If you, as data controllers, are met with a request for access, it will typically be from your employees or customers/potential customers.**Note. If you use Wired Relations as a GRC platform, the systems will be mapped there, and in most cases, you can therefore omit Appendix 1.** |
| --- |

| **Systems** | **System responsible/contact person** |
| --- | --- |
| *HR-system*  |  |
| *Finance-system* |  |
| *Salary-system* |  |
| *E-mail* |  |
| *Storage, etc.* |  |
|  |  |

**Document information**

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