|  |
| --- |
|  **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 securing the rights of data subjects**

**1. Purpose**

This policy concerns the protection of data subjects' rights in accordance with Chapter 3 in the GDPR.

The policy describes how [insert organization’s name here] ensures compliance with data subjects' rights, including how inquiries regarding data subjects’ rights must be handled.

**2. The rights of the data subjects**

This section contains a description of selected rights that are relevant in relation to [insert organization’s name here]'s business practice:

**2.1. The right to information about the processing (obligation to provide information)**

The data subject must be informed about the processing of his/her/their personal data, cf. article 13 and article 14 in the GDPR.

[insert organization’s name here] fulfils the obligation to provide information to customers, business partners and visitors to the website via [insert organization’s name here]' privacy policy, which is available on [insert organization’s name here]' website, and to employees via [insert organization’s name here]' privacy policy for employees, which is available on [insert organization’s name here]' intranet.

**2.2. The right to insight**

The data subject has the right to gain insight into the specific personal data processed about her, cf. GDPR article 15.

The right to insight gives the data subject the opportunity to see what personal data is being processed about the person concerned, and at the same time creates transparency about how the information is processed.

In contrast to the right to insight in the processing (the obligation to provide information), the right to access must be fulfilled in connection with a request for access from the data subject.

Requests regarding the right to access are handled by [insert organization’s name here]'s compliance team, cf. section 3.

**2.3. The right to object**

The data subject has the right to object to processing carried out on the basis of GDPR article 6 (1)(f), even if this is otherwise legal, cf. Article 21 of the data protection regulation.

Requests relating to the data subject's right to object are handled by [insert organization’s name here]'s compliance team, cf. section 3.

**2.4. The right to rectification**

The data subject has the right to have incorrect personal data corrected, cf. GDPR article 16.

The data subject also has the right to have incomplete information made complete, for example by presenting supplementary information in a case.

In addition to the fact that the incorrect personal data must be corrected in the company's own systems, the company must also, on its own initiative, notify those to whom the personal data has been disclosed, so that the personal data can also be corrected there, cf. GDPR article 19.

**2.5. The right to deletion (the right to be forgotten)**

The data subject has the right to have personal data deleted if one of the conditions in the GDPR, article 17(1)(a-f) applies:

* The personal data is no longer necessary to fulfil the purposes for which it was collected or otherwise processed.
* The processing is based on consent, and the data subject now withdraws their consent.
* The data subject objects to the processing in accordance with article 21, and there are no legitimate reasons for the processing that precedes the objection.
* The personal data has been processed illegally.
* The personal data must be deleted in order to comply with a legal obligation in EU law or the national law of the Member States to which the data controller is subject.
* The personal data has been collected in connection with the provision of information society services.
* In addition to the personal data being deleted in the company's own systems, the company must also, on its own initiative, notify those to whom the personal data has been disclosed, so that the personal data can also be deleted there, cf. GDPR article 19.

**2.6. The right to limitation**

The data subject has the right to have the processing of personal data restricted if one of the conditions in the data protection regulation, article 18(1)(a-d) applies:

* The correctness of the personal data is contested by the data subject (in the period until the data controller has had the opportunity to determine whether the personal data is correct).
* The processing is illegal and the data subject opposes the deletion of the personal data and instead requests that its use be restricted.
* The data controller no longer needs the personal data for the processing, but it is necessary for a legal claim to be established, asserted or defended.
* The data subject has objected to the processing in accordance with Article 21, during the period in which it is being checked whether the legitimate interests of the data controller take precedence over the legitimate interests of the data subject.

In addition to restricting the processing in its own systems, the company must, on its own initiative, also notify those to whom the personal data have been disclosed, so that the processing can also be restricted there, cf. GDPR article 19.

**2.7. The right to withdraw consent**

If the processing of the data subject's personal data is based on consent, the data subject has the right to withdraw their consent at any time.

**2.8. The right to complain**

If the data subject is dissatisfied with the processing of their personal data, the data subject can file a complaint or contact the relevant supervisory authority, e.g. the Danish Data Protection Authority.

**3. Procedure for handling requests**

The exercise of several of the above rights takes place in connection with the data subject making a request to [insert organization’s name here].

The procedure below relates to requests that deal with the right to access and the right to deletion, correction and restriction.

A request regarding the rights of data subjects must be answered without undue delay and no later than one month after the request has been made.

**3.1. Receiving requests**

If the data subject wishes to use one or more rights, the employee who receives the inquiry from the data subject must forward the inquiry to the compliance team as soon as possible.

The compliance team can be contacted at [insert email address of contact person in the organization].

3.1.1. Securing the identity of the data subject

The compliance team must initially ensure the identity of the data subject.

If there is doubt about the identity of the data subject, this can be ensured, for example, by presenting ID.

If it is a representative making a request on behalf of the data subject, the compliance team must ensure that a valid power of attorney is available.

In this way, it is ensured that there is no accidental disclosure of personal data to unauthorised persons.

3.1.2. Determining the scope of the request

It must then be assessed whether the request can be answered in its current form, or whether it is relevant to investigate whether the request can be limited, e.g. whether the person wants insight/deletion in relation to a specific area or a specific case.

3.1.3. Finding the personal data

It is initially sought in the company's mapping of the processing of personal data, where the data subject's personal data is processed.

Next, the data subject's personal data is searched in the affected systems in collaboration with the person responsible for the system and/or the IT department.

The procedure in section 3.2 is then followed for requests for insight or section 3.3 of the policy for requests for deletion, rectification or restriction.

**3.2. Requests for insight**

3.2.1. Extraction of the personal data

After personal data has been retrieved, a copy of this is extracted in a readable format.

3.2.2. Assessment of the personal data

The data subject's personal data is reviewed and assessed by the compliance team.

When handing out personal data, it is important to be aware that only information about the data subject must be handed out. If personal data about other data subjects appear, these must be obscured/removed before handing over.

3.2.3 Response to the request

When the compliance team has assessed that the personal data is ready for disclosure, the compliance team will respond to the data subject's request.

In the case of requests for insight, the collected personal data is sent to the data subject via encrypted email or another secure delivery method.

In addition to the fact that the data subject must get a copy of the personal data that is processed about them, the response must also contain information about:

* the purpose of the processing of the personal data
* information about the categories of personal data concerned
* information about the recipients or categories of recipients to whom the personal data is or will be disclosed, in particular if the recipients are located in third countries or are international organizations

In addition, the following must also be disclosed:

* If the personal data are transferred to unsafe third countries or international organizations and necessary guarantees for data protection have been established, the data subject must be informed of these guarantees.
* If possible, information must also be given about the period of time for which the personal data is stored, or, if this is not possible, the criteria used to determine this period of time.
* In addition, the data subject must be informed of their right to request correction, deletion or restriction of the processing, that the data subject has the right to object to the processing in special situations, and that the data subject has the right to lodge a complaint about the processing to a supervisory authority.
* Information must also be given on where the personal data originates from. However, this only applies if the personal data in question have been collected from someone other than the data subject.

**3.3. Requests for deletion, rectification and restriction**

3.3.1. Assessment of the personal data

The data subject's personal data is reviewed and assessed by the compliance team.

*Deletion*

It must be assessed whether one of the conditions in the GDPR's article 17 (1)(a-f) applies, cf. also section 2.5.

If it is assessed that deletion must be carried out, the person(s) responsible for the systems where personal data are found are contacted, and they then delete the personal data in question.

Notification must then be made to those to whom the personal data has been disclosed, so that the personal data can also be deleted there.

*Correction*

If it is assessed that the personal data is incorrect, this should be corrected.

If it is assessed that the personal data is not incorrect, a note must be added stating what the data subject believes to be correct.

Notification must then be made to those to whom the personal data has been disclosed, so that the personal data can also be corrected there.

*Restriction*

It must be assessed whether one of the conditions in the GDPR's article 18(1)(a-d) applies, cf. also section 2.6.

If it is assessed that restriction must take place, the person(s) responsible for the systems where personal data is found is contacted, who then ensures that the processing is restricted.

Notification must then be made to those to whom the personal data has been passed on, so that the personal data can also be restricted there.

3.3.2 Response to the request

When the compliance team has received confirmation that the personal data in question has been deleted, etc. or, when the compliance team has assessed that there are no grounds for deletion, etc., the compliance team responds to the data subject's request.

The compliance team either sends confirmation to the data subject that the personal data has been deleted, etc., or, if there is no basis for deletion, etc., an explanation to the data subject as to why personal data will continue to be processed.

**4. Inquiries regarding assistance in handling requests**

[insert organization’s name here] has entered into data processing agreements with several customers who consider [insert organization’s name here] to be a data processor.

In this connection, [insert organization’s name here] provides assistance to customers in relation to the provision, correction, deletion or restriction of, and information about, the processing of personal data to the data subject.

Requests for this are handled by the compliance team in accordance with this policy as well as the entered into data processing agreements, including the deadlines stipulated in the data processing agreements, to the extent possible.

**Document Information**

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