Note that this template includes legal provisions for Germany by referencing the German Federal Data Protection Act (BDSG). If your company is based anywhere else, you should customize the contents before using the template.

# Data Protection and Confidentiality Agreement

As part of your employment, you may be instructed to process personal data or potentially personal data that has been entrusted to you in accordance with the data protection regulations. To that end, you are provided with an overview of the regulations relevant to your obligation. Data which you have become aware of during the performance of your duties must not be misused for your own or any other purposes. This obligation remains in force even after the termination of your employment. Deliberate or negligent breaches can have legal consequences.

Personal data is all information related to an identified or identifiable person. It may not be collected, used, passed on or otherwise processed without authorization. Personal data may only be processed in line with company instructions. In addition to instructions from a supervisor, the following are regarded as instructions: documents of the company"s quality management system, other operational documentation, flow charts, company agreements or employee manuals.

---

I, <employee name>

hereby commit to keep strictest confidentiality with respect to personal data and to process it exclusively according to the instructions of <enter company name>. I hereby further commit to keep strictest confidentiality with respect to the personal data I shall collect, process, or access in the scope of my activities for <enter company name>, and to refrain from disclosing them to any other natural or legal person, including other employees of <enter company name>, unless disclosure is explicitly authorized by instructions of the employer, contract or law, or unless disclosure is necessary to fulfill the instructions of <enter company name>.

For instance, I am not allowed to use mobile data media, take printed copies home with me, or pass on personal passwords to third parties. Further instructions on what has to be observed in terms of data protection law can be found, inter alia, in:

- The company"s technical and organizational measures
- Company forms on employee obligations with regards to the handling of hardware
- The company"s list of data processing activities

- <add anything else relevant here, e.g. authorization concept for software systems>

This non-disclosure and confidentiality obligation continues to apply even after my employment with <enter company name> has ended.

I am aware that any infringement against this obligation or of applicable data protection law such as Art. 83 of the European General Data Protection Regulation (GDPR), §§ 42 and 43 of the German Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG) or other applicable European or national legal provisions may result in serious fines, monetary or prison sentences and may possibly cause damage to natural or legal persons, including the employer. In addition, infringement against this obligation may also constitute a breach of obligations under the employment contract or of specific obligations for confidentiality and may, for example, lead to a formal warning, a termination in due time or without notice or to an obligation to pay for compensation. Legal consequences of a breach can also entail claims for damages against me personally by the persons to whom such data refers. In these cases, I may be liable without limitation with all my assets and without the possibility of residual debt discharge in the course of insolvency proceedings. Other obligations of secrecy, such as those arising from the employment contract, continue to exist alongside this obligation.

I have read and understood this obligation to maintain confidentiality and to comply with data protection regulations:

<Place, date and signature of employee>
<Place, date and signature of supervisor>

I confirm that I have been informed about the meaning and relevance of this data protection obligation. I have been given the opportunity to receive a copy of this form as well as further information on data protection and the text of Art. 29 GDPR, Art. 83 para. 4 - 6 GDPR, Art. 42 para. 1 and 2 BDSG and Art. 43 para. 1 and 2 BDSG.

<Place, date and signature of employee>
<Place, date and signature of supervisor>

---

## Annex: Further information on data protection

- **Processing** within the EU General Data Protection Regulation (DSGVO) means any process or series of operations performed with or without the aid of automated processes in connection with personal data such as collection, organization, ordering, storage, adaptation, alteration, reading, querying, use, disclosure through transmission, dissemination or other form of provision, matching or linking, restriction, erasure or destruction. Any processing of personal data must be carried out according to a valid legal

basis out of those recognized by art. 6 GDPR and only for the purpose they have been collected for.

- **Personal data** within the meaning of the GDPR are all information relating to an identified or identifiable natural person; a natural person is considered as identifiable if it can be directly or indirectly identified, in particular by association with an identifier such as a name, an identification number, location data, an online identifier or one or more special features, the expression of the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person. The principles of the European General Data Protection Regulation (GDPR) for the processing of personal data must be adhered to; they are laid down in Art. 5 para. 1 GDPR and essentially contain the following obligations.

Personal data must be

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

**Art. 29 GDPR: Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

**Art. 83 GDPR: General conditions for imposing administrative fines**

(4) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10.000.000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

1. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
2. the obligations of the certification body pursuant to Articles 42 and 43;
3. the obligations of the monitoring body pursuant to Article 41(4).

(5) Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

1. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
2. the data subjects" rights pursuant to Articles 12 to 22;
3. the transfers of personal data to a recipient in a third country or an international organization pursuant to Art. 44 to 49;
4. any obligations pursuant to Member State law adopted under Chapter IX;
5. non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

**§ 42 BDSG: Penal provisions**

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. transferring the data to a third party or
2. otherwise making them accessible

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. processing without authorization, or
2. fraudulently acquiring

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

**§ 43 BDSG: Provisions on administrative fines**

(1) Intentionally or negligently engaging in the following shall be deemed an administrative offense:

1. in violation of Section 30 (1) failing to treat a request for information properly, or
2. in violation of Section 30 (2), first sentence, failing to inform a consumer or doing so incorrectly, incompletely or too late.

(2) An administrative offense may be punished by a fine of up to fifty thousand euros.

---