**Model for the documentation of a processing activity
pursuant to Article 30 GDPR**

|  |  |
| --- | --- |
| **Description of the processing activity** | *The name should briefly and concisely describe which processing is meant. Examples: Personnel administration, accounting, administration of project data, handling of application data, project management, organisation of training courses, etc.*  |
| **Purpose of the processing** | *Why do you process the data? What is the purpose of the processing?**Examples:* * *Data processing in the employment context*
* *Ensuring the operation of the organisation or company*
* *Ensuring general safety measures*
* *Provision of infrastructure for the operation of the organisation or company*
* *Establishment, execution or termination of purchase or service contracts*
* *Manufacture of products and services*
 |
| Responsible department | *Which department in your organisation or company is responsible for processing?*  |
| Contact person | *Appoint an internal contact person or the person responsible for the process (business process owner).* |
| Process description | *Brief description of the processing. (optional)**Describes the internal process in brief. This is only for illustration and better understanding.* |
| Groups of people affected | *List the categories of persons affected by the processing. Possible categories are e.g.* * *Employees*
* *Interested parties*
* *Suppliers*
* *Customers*
* *...*
 |
| Categories of data concerned | *List the categories of personal data of the data subjects that are processed in the context of this processing.* *You should take your time here and carefully consider which data you process from the data subjects. This depends heavily on the processing in question.* *e.g. (Please specify as far as possible)** *Personal master data (e.g. name, date of birth, marital status, etc.)*
* *Contact details (e.g. postal address, e-mail address, telephone number, etc.)*
* *Employee master data (e.g. income tax class, personnel number, etc.)*
* *Usage data (e.g. surfing behaviour, purchasing behaviour, access data, etc.)*
* *Contract data (e.g. contract number, contract contents, billing modalities, etc.)*
* *Identification features and identification numbers (e.g. identity card number, passport number, tax number, etc.)*
* *Payroll data for personnel (e.g. wages/salary, bonuses, health insurance contributions, other deductions, etc.)*
* *Customer data (e.g. conditions, order history, payment behaviour, etc.)*
* *Payment data (e.g. bank details, credit card details, etc.)*
* *Application-specific data (e.g. certificates, application documents, etc.)*
* *Supplier data (contact persons and their contact details, etc.)*
* *Imposed data (data that the data subject provides of their own accord)*
* *....*
 |
| Special personal data | **Are special categories of personal data processed in accordance with Art. 9?** *Yes / no**The GDPR defines particularly sensitive data in Article 9. If you process such data, we strongly recommend that you carry out a data protection impact assessment (DPIA). You should also consult a data protection expert or legal advisor.* *Note: This concerns "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (data according to GDPR Art. 9 (1))* |
| **Categories of recipients to whom the personal data have been or will be disclosed (pursuant to Art. 30 (1) d) GDPR)** |
| Internal receivers | *List of internal recipients (e.g. individual departments or groups of people)**e.g.** *Accounting*
* *Management*
* *IT department*
* *Other recipients in case of need*
* *...*
 |
| External receivers | *External recipients are primarily service providers or authorities that either have access to the data or to which the data is transmitted. The providers of software solutions that theoretically have access to the stored data are also listed here.* *e.g.** *Tax consultant*
* *Service provider XYZ (state name and type)*
* *...*
 |
| Data transfer to third countries(pursuant to Art. 30 para. 1 e) GDPR) | *Record here whether the data is transferred to a third country. This often happens when using service providers (especially internet service providers and software solutions from the cloud).* *For this point, either state: "Data transfer does not take place and is not planned." or "Data transfer to a third country takes place." and then describe which transfer takes place.* *Note: The third country should always be specified here as soon as it is not the country in which you are based. You can also specify the place of data processing and the headquarters of the service provider (if different).* *A risk assessment of the third country must also be carried out.* *All EU countries and countries that have been recognised by the EU as having an adequate level of data protection through an adequacy decision are uncritical. Further measures should be implemented for all other countries.* *The corresponding guarantees should also be listed here. At the very least, a contract for commissioned data processing should be concluded with the respective service provider.*  |
| Deadlines for the deletion of data | *Record when you delete the recorded data. Here you can also refer to an external deletion concept, which must be created separately.*  |
| **Data protection compliance check for data controllers** |
| Legal basis of the processing activity  | *The processing of personal data is only lawful if one of the legal bases listed in the GDPR is applicable:** *The processing is based on the consent of the data subject (GDPR Art. 6 para. 1 a)*
* *The processing is necessary for the fulfilment of a contract or for the implementation of pre-contractual measures. (GDPR Art. 6 para. 1 b)*
* *Processing is necessary for compliance with a legal obligation. (GDPR Art. 6 para. 1 c)*
* *Processing is necessary to protect vital interests. (GDPR Art. 6 para. 1 d)*
* *Processing is necessary to protect the public interest. (GDPR Art. 6 para. 1 e)*
* *The processing is based on the legitimate interest of the controller. (GDPR Art. 6 para. 1 f)*
 |
| Further laws | *If there are other laws in your country on the basis of which you carry out the processing described here, you can document them here.*  |
| **Description of the technical and organisational measurespursuant to Art. 30 para. 1 g) in conjunction with Art. 32 para. 1 GDPR***To ensure the protection of personal data, you must define technical and organisational measures in your company. These can also be documented separately.*  |