Instructions on preparing the record of data processing activities (art. 30 GDPR)

[condensed summary of the instructions issued (in German) by the German Data Protection Conference (*Datenschutzkonferenz)* which can be downloaded on the website of the Federal Commissioner for Data Protection and Freedom of Information (status: 25 April 2018):

"*Hinweise zum Verzeichnis von Verarbeitungstätigkeiten*", https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html]

For purposes of illustration the following instructions include lists of examples. Please note that such lists of examples are not exhaustive.

1. Scope of application / exceptions

Each person responsible and each contracted data processor (*Auftragsverarbeiter*) must establish and maintain a record of all personal data processing activities.

As an exception, pursuant to art. 30 para. 5 GDPR companies/contracted data processors with less than 250 employees are exempt from the obligation to maintain a record of their data processing activities. This exception does however not apply in case that they carry out data processing operations that:

- are likely to result in a risk to the rights and freedom of data subjects (e.g. scoring for credit rating, fraud prevention measures, video surveillance, GPS based tracking of employees, processing of communication etc.);
- include special categories of data as referred to in art. 9 para. 1 GDPR (data revealing religious beliefs, health data, biometric data etc.) or personal data relating to criminal convictions and offences as referred to in art. 10 GDPR;
- or that are not occasional (any other processing activities such as for example payroll accounting, client data administration, IT/internet/e-mail protocols etc.).

With regard to regular payroll accounting/client data administration most companies will not be exempt from the obligation to maintain a record of their processing activities, even if they employ fewer than 250 persons.

2. Purpose of the record

For each individual data processing activity, a description according to art. 30 GDPR must be provided. The record of data processing activities therefore can be described as the sum of all individual data processing activity descriptions.

The record of data processing activities is only one of several elements that are necessary to meet the accountability obligation stated in art. 5 para. 2 GDPR. In addition, companies must also be able to prove the existence of any declarations of consent (art. 7 para. 1 GDPR), the general lawfulness of the data processing (art. 24 para. 1 GDPR) as well as the result of any privacy impact assessment (*Datenschutzfolgenabschätzung*, art. 35 para. 7 GDPR) by appropriate documentation.

To avoid redundancies and repetitions, it is possible to refer to other existing documents, in particular any documents that have been established in connection with the company's general information security management.

Each person responsible and each contracted data processor is obliged to cooperate with the competent data protection authorities and, upon demand, present the record of data processing activities to them.

Moreover, the record of data processing activities can also be used to ensure compliance with other data protection obligations, e.g.:

- determination of the purposes of the processing according to art. 5 para. 1 lit. b GDPR;
- for accountability and documentation purposes according to art. 5 para. 2, art. 24 GDPR;
- as an appropriate instrument to be able to provide information to the affected data subjects according to art. 12 para. 1 GDPR;
- as a basis for the tasks of the DPO according to art. 39 GDPR;
- for purposes of examination whether a privacy impact assessment must be executed.

If the person responsible/the contracted data processor wants to use the record for such additional purposes, it is appropriate and reasonable to include additional information, e.g. individual data fields, origin/source of the data, legal basis of the processing, responsible employees, persons/groups of persons having access to data etc., in the record.

3. Presentation of the record to the authorities

Upon demand, the record must be submitted to the authorities (art. 30 para. 4 GDPR). The authorities must be able to check the data processing operations based on the descriptions and information included in the record. In case that the authorities limit their examination to certain processing operations, only the relevant parts of the record must be presented.

4. Form of the record

4.1. Language

As a rule, the record must be drafted in German. In any case the company must be able to present a German version of the record without delay upon demand of the authorities.

4.2. Written/electronic form

The record must be established “in writing” (including in electronic form) accordingly to art. 30 para. 3 GDPR. In case that the record is maintained in electronic form, the authorities may nevertheless request the submission of a printed version (where appropriate limited to only certain parts of the record).

5. Regular updates – history of modifications

To be able to retrace modifications (e.g. names of past DPOs etc.), changes shall be documented and the documentation shall be stored for a retention period of at least one year. This follows from the obligation of accountability in art. 5 para. 2 GDPR.

6. Content of the record – person responsible (art. 30, para. 1 GDPR)[1]

The record must contain all information referred to in art. 30 para. 1 sentence 2 lit. a) to g) GDPR. The information provided in the record must be clear and conclusive. It is recommended to define a title for each processing activity based on the respective purposes for processing, e.g. “administration of employee data/master data” or “payroll accounting”.

6.1. Name/contact details

(postal address, electronic contact details, phone number)

- of the person responsible
- of a joint controller (art. 26 GDPR), if applicable
- of the representative if the processor is not established in the EU (art. 27 GDPR)
- of the DPO, if applicable

The information shall enable the authorities to easily and quickly join the person responsible, notably if there is an urgency.

Regarding legal persons, it is recommended by the authorities to directly indicate the person who is operationally responsible (if different from the legal representative).

6.2. Purposes of processing

For each description of a processing activity the purposes of the processing must be defined and documented accordingly, e.g.:

- Employee records/master data
- Payroll accounting
- Time sheets/recording of working hours
- Holiday planning
- Recording of IT/internet/e-mail use
- Application process
- Recording of phone data
- Video surveillance of work places
- Purchasing/procurement
- Financial accounting.

[1] Regarding the content of the records to be established and maintained by a contracted data processor (*Auftragsverarbeiter*), see below, art. 7.

6.3. Categories of data subjects and personal data

The various categories of data subjects and personal data must be described accordingly. It is recommended to assign a serial order number to each category of personal data in order to allow for a quick and simple allocation to other information referred to in art. 30 GDPR, e.g. the respective time limits for deletion of data.

Example: Data subject category “Employees”, various categories of personal data:

1) Employee master data (address, date of birth, tax details, working hours, qualification, bank account, function, …)
2) Application details including contact details, information on the applicant’s qualifications and activities etc.
3) Employer references including address data, performance data etc.
4) Warning notices including address data, work behaviour etc.
5) Video surveillance at the work place

Example: Data subject category “Clients”, various categories of personal data:

1) Contact details, address data, contact persons etc.
2) Client group/interests
3) Sales data
4) Creditworthiness
5) Payment details

6.4. Categories of data recipients

The categories of data recipients to whom the personal data have been disclosed in the past or will be disclosed in the future must be indicated (including recipients in third countries or international organisations).

Example of categories of possible data recipients for the processing activity “Payroll accounting”:

- Banks
- Social security bodies
- Tax authorities
- Internal data recipients, e.g. company doctor, works council
- Parent company
- Contracted data processors
- Creditors (e.g. in case of attachment of salaries)
- Pension providers

It is recommended to not only provide information regarding “data recipients” (as requested by the wording of the GDPR), but also regarding persons who have access to personal data (*Zugriffsberechtigte*). This does however only require details on the function/role of such persons, not their names.

In any case, the record shall include information about the eventual transfer of data to a third country (e.g. server located in a third country, administration of e-mail communication via a third country, execution of support services in a third country,

etc.) – even if such transfer does not take place/is not planned, this shall be stated in the record.

6.5. Transfers to a third country

This section requires information regarding the transfer of data to third countries/international organisations, including the indication of the respective country/organisation. In case of a data transfer to a third country according to art. 49 para. 1, subpara. 2 GDPR, the record must further include the documentation of "suitable safeguards".

6.6. Time limits for data erasure

It is necessary to precisely indicate the time limits for the deletion of the different data categories, e.g.:

- applicable legal/tax retention periods for employee/client data
- legal deletion periods
- review and deletion periods fixed by the person responsible

6.7. Technical and organisational security measures as referred to in art. 32 para. 1 GDPR

Pursuant to art. 5 para. 2 GDPR, the person responsible is obliged to document the technical and organisational measures used to ensure appropriate security of personal data. Moreover, such measures must be regularly reviewed for their effectiveness. This however requires that the technical and organisational measures have been comprehensively described beforehand.

Examples of technical and organisational measures (TOM) resulting from art. 32 para. 1 GDPR:

- Pseudonymisation of personal data, e.g.
  - definition of pseudonymisation rules,
  - determination of data to be replaced by pseudonymisation,
  - protection of secret parameters,
  - determination of the persons who shall be authorised to carry out pseudonymisation/de-pseudonymisation procedures

- Encryption of personal data, e.g.
  - determination of the persons who shall be authorised to access/administrate encryption keys,
  - random generation of encryption keys,
  - protection of encryption keys,
  - regular change of encryption keys

- Ensuring the integrity and confidentiality of systems/services, e.g.
  - development of mandatory security directives
  - definition of responsibilities
  - inventory of IT equipment
  - inventory of processed personal data

- raising awareness for data protection matters among employees, training of employees
- implementation of a defined roles and authorisations concept

- Ensuring the availability and resilience of systems/services, e.g.
  - preparation of backup copies and transaction histories, configuration measures etc. according to a tested concept,
  - protection from external factors (malware, sabotage, force majeure),
  - repair strategies,
  - substitution rules (for absent staff)

- Recovery of personal data and access to such data after a technical/physical incident, e.g.
  - preparation of an emergency plan/emergency manual,
  - performance of emergency exercises

- Implementation of procedures to regularly review, assess and evaluate the effectiveness of the above-mentioned measures, e.g.
  - sharing information on newly discovered risks/flaws,
  - regular revision of the security concept,
  - regular compliance audits by the DPO/IT department,
  - external audits/certification

6.8. Further recommended measures

The wording of art. 32 GDPR *"[…] shall implement appropriate technical and organisational measures […] including inter alia*" illustrates that the list of measures referred to is not exhaustive. Therefore, it is recommended to also include a description of the following:

- measures to ensure the strict purpose limitation of personal data (art. 5 para. 1 lit. b) GDPR), e.g.
  - limitation of access/processing/transfer rights
  - closure/avoidance of interfaces (in procedures/software)
  - software development compliance/quality assurance measures

- measures to ensure transparency (vis-à-vis the affected data subjects/persons responsible/supervising bodies, e.g.
  - documentation of procedures
  - documentation of tests, preliminary assessments of newly introduced or modified procedures
  - documentation of consent declarations/objections
  - logging of accesses and modifications
  - documentation of contracts with external service providers
  - documentation of data sources

- measures to guarantee the rights of the affected data subjects (art. 13 et seqq. GDPR), e.g.
  - implementation of standardised interfaces for the exercise/enforcement of their rights/claims
  - implementation of standard procedures and possibilities to compile/delete/limit/correct personal data

- implementation of consent/withdrawal/objection procedures

6.9. Reference documents

It is recommended to indicate further elements at the end of the documentation (for example under “miscellaneous”) to ensure a comprehensive documentation of the data protection strategy, e.g.:

- internal rules of behaviour
- documentation of any risk analysis or general description of data security
- general data security concept
- certificates
- results of privacy impact assessments

7. Content of the record – contracted data processor (art. 30, para. 2 GDPR)

Like the person responsible, any contracted data processor (*Auftragsverarbeiter*) is obliged to establish and maintain a record of data processing activities which, in this case, must contain all information referred to in art. 30 para. 2 GDPR, including all clients/missions as well as any subcontractors.

Subcontractors must only indicate their direct clients, not the entire “chain” of contractors back to the person responsible.

8. Violations/sanctions

Any violation consisting in

- the failure to maintain a complete record of data processing activities or
- the failure to submit the record to the authorities upon request

shall be subject to administrative fines up to 10.000.000 EUR or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (art. 83 para. 4 lit. a) GDPR).