Deloitte.

URL: http://mobile.deloitte-tax-news.de/german-tax-legal-news/the-new-records-of-data-processing-activities.html

21.11.2016

German Tax and Legal News

The new records of data processing activities: What are the requirements of the EU-GDPR?

EU General Data Protection Regulation: New legal requirements for the records of data processing activities

As of May 2018, the EU General Data Protection Regulation (GDPR) applies. Until then data processing operations need to be adapted to the new requirements. We provide you with important information on the new records of data processing activities.

The GDPR stipulates broad requirements regarding the documentation and proof of compliance. In future, controllers have to prove that their data processing operations meet the requirements of the GDPR (accountability).

The records of processing activities, subject to Article 30 GDPR, are one important part of the privacy documentation. They are similar to the procedure index already known from German Privacy Law (BDSG).

What is new?
There are quite a few changes under Article 30 GDPR.

To start with, the GDPR provides that only enterprises employing 250 employees or more have to keep a record of processing activities. However, this obligation also applies to smaller enterprises if

- the processing is likely to result in a risk to the rights of affected employees (e.g. scoring, comprehensive monitoring, high risk resulting out of unauthorized disclosure or access, use of new technologies),
- the processing is not occasional or
- the processing includes special categories of data as referred to in Article 9 (1) (e.g. health data, biometric data, data related to political or philosophical beliefs) or personal data relating to criminal convictions and offences referred to in Article 10.

Therefore, also a lot of small and medium size enterprises will be obliged to keep the records.

Another novelty is that the GDPR does not distinguish between the internal and the external records anymore. There is now only one kind of record: the internal record. Upon request, it has to be made available to the supervising authorities.

Finally, if the requirements are not met, an administrative fine of up to EUR 10 Million or up to 2% of the annual global turnover may be imposed, Article 83 (4) GDPR.

What are the requirements regarding the content?
With respect to the content, the record has to provide general information:
Name and contact details of the

- controller,
- controller's representative (owner, management, CIO),
- EU-Representative, if the controller is not established within the EU,
- Data Protection officer.

Additionally, cross-procedural technical and organizational information has to be provided:

- Description of the technical and organizational measures to protect personal data according to Article 32 (1) GDPR,
- erasure concept.

Finally, specified information on the separate data processing operations has to be provided:

- Name of the data processing operation,

- purposes of the processing,
- categories of data subjects,
- categories of personal data,
- categories of recipients to whom the personal data have been or will be disclosed (internal and external),
- categories of recipients in third countries or international organizations

► recipient,
► third country or organization,
► sufficient guarantees for the protection of the data and the rights of the data subjects in the third country or the international organization,

- erasure period,
- if applicable: special data protection measurements.

In case of commissioned data processing, in addition to the general information on the controllers, information on the commissioned data processor has to be provided.

What are the requirements regarding the form?
The records of processing activities shall be in writing or in electronic form.