

CO.25 Network and Information Security

Authors: Winfried Veil

Last update: 2021-06-11 09:06:01 | By: Winfried Veil

Created at: 2021-05-12 12:06:01

Rec. 49 GDPR clarifies that network and information security can be a justification for the processing of personal data:

“The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.”

The term "information security" can be found primarily in the **BSI's** basic **IT-Grundschutz catalogs** and in **ISO/IEC 27001**. There, it has the protection of information as its goal. Unlike data protection, it is irrelevant for information security whether automated data processing takes place and whether the data has a personal reference. In some cases, data security [**Tile O.15**] is regarded as a part of information security because the latter is more comprehensive.