

BC.02 Risk

Authors: Winfried Veil

Last update: 2021-05-22 14:23:11 | By: Winfried Veil

Created at: 2021-05-12 20:57:36

82 provisions of the GDPR contain the obligation to carry out a balancing decision [\[Tiles BD\]](#). The standards according to which these assessments are to be carried out remain unclear in many cases.

One balancing criterion is undoubtedly the risk (risk-based approach). It should be noted that this is not about the risk for the controller, i.e. the business risk, but about the risk for the data subject. Numerous provisions stipulate that the controller must determine the risk to the rights and freedoms of the data subject and put it in relation to the measures to be taken by the controller:

Articles: 4 No. 24, 23 II g, 24 I, 25 I, 27 II a, 30 V, 32 I/II, 33 I, 39 II, 34 I, 34 III b, 34 IV, 35 I, 35 VII c/d, 35 XI, 36 I/II, 39 II, 49 I a, 57 I b and 70 I h GDPR.

Recitals: 9 (1), 28 (1), 38 (1), 39 (5), 51 (1), 71 (6), 74 (3), 75 (1), 76, 77, 80 (1), 81 (3), 83, 84, 86 (1)/(4), 89 (3), 90, 91 (1)/(3), 94 (1)/(2)/(5), 96, 98 (2) and 122 (3) GDPR.

To what extent the risk-based approach has to be applied in the GDPR as a whole (i.e. beyond the provisions mentioned above) is disputed.

Some GDPR provisions can be readily understood to mean that the risk to the data subject must also be taken into account (see, for example, Article 6 IV d GDPR, according to which the "possible consequences of the intended further processing" for data subjects must be included in the assessment). For many other legal terms (such as fairness, proportionality, purpose of processing, etc.), the inclusion of risk considerations is obvious.

Having to determine the risks of processing in a particular case, means that you have to determine the *Schutzgut* for which a risk should exist. This assessment prevents data protection from becoming an end in itself. The technical and organisational measures to be taken cannot be calibrated in a risk-adequate manner without also affecting the legal obligations that are to be fulfilled by the technical and organisational measures.

In English-language literature, there is therefore even talk of a "risk revolution" (Claudia Quelle) or a "riskification" of data protection law (Milda Macenaite).

Literature on the risk-based approach under [Tile L.02](#).