C.11 Preventive State

Authors: Winfried Veil

Last update: 2021-06-06 23:14:53 | By: Winfried Veil

Created at: 2021-06-05 14:24:16

Paradoxically, the GDPR creates the preventive state that it actually wants to prevent. The preventive state refers to a state that is committed to the early detection and reduction of possible threats to the state and its citizens and that uses information and state-controlled instruments in a targeted and comprehensive manner to prevent undesirable behaviour by citizens from the outset.

The term "preventive state" originates from the policy debate on security legislation, the aim of which is to fight terrorism and crime. The preventive state under data protection law has similar structural elements to that preventive state:

> *? In the preventive state of data protection law, every controller is regarded as a potential risk (general suspicion). Some advocates of data protection law even believe that a generalised attacker model applies in data protection: "Every organisation, especially one that is legally authorised to process data, is an attacker!" (cf. Martin Rost, **Künstliche Intelligenz trifft Datenschutz**) This view has great similarities with the figure of the **"Gefährder"** - a term that is used in Germany in the law of* prevention of threats to public security *since 2004 to describe a "dangerous person", which has not yet committed any criminal offences, but for whom "certain facts justify the police authorities' assumption that they will commit criminal offences of considerable importance".*

> *? In the preventive state of data protection law, the creation of even the most remote risk of legal impairment through data processing is already subject to extensive formal and material obligations, even before the person responsible is even allowed to begin processing the data. Causing a violation of a legal interest or damage is no longer relevant.*

> *? In the data protection prevention state, the data protection supervisory authorities do not have the authority to collect the information necessary for their surveillance activities using police or secret service methods. However, the GDPR obliges controllers to do this themselves. Comprehensive documentation obligations ultimately force them to record every processing step and every technical and organisational measure. Comprehensive accountability obligations force them to be able to prove his measures at any time. The purpose of this "accountability" is to facilitate state control - a classic approach of the preventive state.*

> *? In the data protection preventive state, the GDPR protects all "rights and freedoms of natural persons" (Art. 1 II GDPR). Thus, the "Schutzgut" or the "Schutzgüter" of the GDPR are unclear (see Tiles **R.01**, **DS.01**, **CO.01** and **P.01**). With this breadth of potential*

> *"Schutzgütern" (i.e. protected rights and interests), it is unclear for every user of the law what the standard for the legality test is. This is also a parallel to the preventive state under security law. The object of protection pursued can no longer be named precisely. It is no longer a matter of averting a concrete danger.*

To shift the measures against dangers and risks to a stage where the danger/risk is still very abstract becomes a problem of the rule of law. The state then no longer relies on its citizens behaving in accordance with the norm. On the contrary, the threshold for intervention is lowered. It is no longer a question of a concrete danger to a sufficiently specific legal asset. The aim is rather to be able to control citizens as comprehensively as possible. The GDPR pursues this goal with its numerous information, documentation and verification obligations.

More about the preventive state of data protection, see *Veil*, **Datenschutz, das zügellose Recht – Teil IV: Der Präventionsstaat** (in German).