

## C.20 Paternalism

Authors: Winfried Veil

Last update: 2021-06-06 22:59:33 | By: Winfried Veil

Created at: 2021-06-06 20:39:37

### Central concern of data protection law: self-determination

A central concern of data protection law is the protection of informational self-determination [[Title GL.02](#)]. In the [diction of the German Federal Constitutional Court](#) this is

*"the power of the individual to determine in principle for himself the disclosure and use of his personal data."*

The aim is thus to achieve the highest possible degree of self-determination.

If one understands self-determination in the sense of case law as personal autonomy and as the right of the individual to be subject in principle to no restrictions in evaluations of what is good or bad for one's own person, healthy or unhealthy, reasonable or unreasonable, and to be subject to no compulsion to an objective rationality, the question arises as to whether data protection law can fulfil its promise to guarantee the individual a maximum of self-determination.

### Paternalism instead of self-determination

Many of the provisions of the GDPR "in themselves" serve self-determination. However, they replace - to put it charitably - the genuine self-determination of the individual with something that can be regarded as "well-understood" (i.e. in the sense of the lawmaker "well-understood") self-determination. Maliciously expressed, one will have to speak of "data paternalism".

Paternalism is to be understood here as any state measure that has the goal of improving the situation of citizens and that is undertaken contrary to or in disregard of autonomously made decisions of the beneficiaries to act or not to act. This article is largely based on an essay by *Christoph Krönke* ([Datenpaternalismus, in: Der Staat 55 \(2016\), 319](#)).

## Form of consent

Consent [\[Title O.03\]](#) may be regarded as a genuine expression of self-determination. However, the GDPR places high demands on the effectiveness of consent:

? *Consent must be given for the specific case: Art. 7 II; Rec. 32 (1)/(4)/(5) and 43 (2) GDPR.*

? *Consent requires that the person giving consent is informed: Rec. 32 (1)/(4) and 42 (4) GDPR.*

? *Consent must be given by an unambiguous indication of the data subject's agreement: Rec. 32 (1) GDPR.*

? *In certain cases, consent must even be given explicitly (e.g. in the case of sensitive data or automated individual decision-making): Art. 9 II a, 22 II c and 49 I a GDPR.*

? *The controller must be able to demonstrate that the data subject has consented: Art. 7 I GDPR.*

**Indirect compulsion:** All these requirements lead to an *indirect compulsion to legal formality*. Because even if no form is explicitly prescribed, the obligation to document leads in practice to the fact that the controller will, in case of doubt, obtain the consent in writing and with signature(s). For example, the consent of the legal guardians for the class photos of their child is regularly obtained on corresponding forms.

**Without an increased need for protection:** The legal system does have formal requirements for legal transactions (e.g. the obligation for notarisation in the case of property purchase contracts). However, these are justified by an increased need for protection of legal transactions or the parties involved compared to the normal case. In the case of consent, however, the legal formality requirement is the normal case ([Art. 7 I GDPR](#)). In the case of sensitive data, the formality requirements are raised even higher ([Art. 9 II a GDPR](#)).

**Effect on the will of the data subject:** The *de facto* formality requirement for consent goes far beyond the degree required by Sections 133 and 157 of the German Civil Code (BGB) for the interpretation of ordinary declarations of intent in legal transactions or acts similar to transactions. The high requirements of the GDPR can very easily lead to a discrepancy between the actually exercised and the legally recognised will of the data subject.

**"Voluntary dissonance":** For example, the "definiteness" or "informedness" of consent on social media such as *Facebook*, *WhatsApp* or *Twitter* often has legal deficiencies from the perspective of the supervisory authorities - with the consequence that the consent is invalid and the data processing is unlawful. However, as can be seen from the persistently high usage rate of these services, which are

controversial from a data protection perspective, most data subjects do not see this as a problem. Their decision is nevertheless in favour of the services. From the point of view of the supervisory authorities, these are wrong decisions. But that is precisely why we speak of paternalism here.

## **Voluntariness of consent**

The voluntary nature of consent required by the GDPR can also come into conflict with the clearly expressed will of the data subject. Although it is controversial whether the GDPR

*? contains a strict prohibition of tying (in which case the performance of a contract should not be made dependent on consent if it is not necessary for the performance of the contract) or whether*

*? [Art. 7 IV GDPR](#) "only" contains an obligation to "take account of a fact" (in which case the fact that consent is not necessary for the performance of the contract must only be taken into "utmost account").*

In any case, the validity of consent is determined according to objectively-typified criteria. The question of whether the data subject actually gave consent of his or her own free will is irrelevant. In other words:

*Even if I wanted it as much as I could and I felt as free as I did: self-determination contrary to the legal assumption of involuntariness would then not be possible.*

This, too, bears paternalistic traits.

## **Purpose Limitation**

A prime example of paternalistic regulation is the principle of purpose limitation [[Title PC.09](#)]: personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes ([Art. 5 I b GDPR](#)).

**Abdicability?** It is completely unclear whether and to what extent this principle can be waived at the request of the data subject. It would be conceivable, for example, that a data subject provides personal

data to science by way of data donation and explicitly waives the right to use the data only for specific purposes.

**Ethical standards of scientific research:** However, the mention of so-called broad consent in [Rec. 33 GDPR](#) speaks against the waiver of the principle of purpose limitation. According to this, data subjects may give their consent for certain areas of scientific research if this is done in compliance with the recognised ethical standards of scientific research. Conversely, this means that even in the case of scientific research, a complete abandonment of purpose limitation, even with the informed consent of the data subject, is out of the question.

## Data Protection by Default

Art. 25 II GDPR requires data protection by default.

**Preventive interest by default:** This provision does not represent "hard" paternalism, because a data protection-friendly default setting can be reversed at any time. However, a legal obligation to protect data by default temporarily relieves citizens of another decision they have to make on their own responsibility. Instead of leaving it to the free play of forces which default setting is chosen for data processing, the state carries out a typified weighing of interests in favour of the (supposed) prevention interest of the data subject. In case of doubt, the "independent data protection supervisory authority" - i.e. the state - decides what is more "data protection-friendly" when choosing between different setting options.

**Without actual will:** Regardless of a possibly opposing will of the data subject, the data subject must always first actively overcome the state-enforced data protection-friendly default settings in order to enjoy the data processing.

**"Nudging" the inertia of the masses:** With this provision, the legislator is taking into account the "inertia effect" that can be proven in behavioural psychology. The result of this provision should therefore also be that, by and large, data protection-friendly default settings will no longer be changed. This is not intrusive paternalism, but "nudging" - the younger sister of paternalism:

*Irrespective of the concrete circumstances of processing, irrespective of the concrete risk for the data subject and irrespective of the fundamental rights affected on the side of the controller, the standard-setter carries out a balancing of interests that is predetermined for all cases.*

## Necessity in the context of contractual constellations

According to [Art. 6 I b GDPR](#), the processing of personal data is permissible if it is necessary for the performance of the contract. [For the necessity tests of the GDPR, see [Tile BD.06](#)].

**EDPB approach:** according to the *European Data Protection Board* ([Guidelines 2/2019](#), para. 30), the term "necessary" should be interpreted objectively:

*"[...] it is required that the processing is objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject."*

**Core of a contract:** For this purpose, the "core of a contractual agreement" must be determined, which does not have to be identical to the contractual clauses. Then it must be examined whether the data processing is necessary for the objectively determined contractual purpose, whereby a strict proportionality standard applies (on the whole, *Malte Engeler*, [The EDPBs guidelines 02/2019 on Art. 6\(1\)\(b\) GDPR, in: PinG 04/2019](#)).

**GDPR vs. freedom of contract:** The EDPB apparently assumes that

? *the GDPR goes beyond the limits of contract law when interpreting declarations of intent,*

? *the actual contractual clauses can be disregarded; and*

? *data protection law principles (such as the fairness principle of [Art. 5 I b GDPR](#)) can be used to identify a genuine data protection law contract content.*

**Primacy of contractual interpretation under data protection law:** Private autonomy and freedom of contract [see [Tile CO.19](#)] are replaced by contractual interpretation under data protection law. However, the data protection supervisory authority does not only claim to control the "small print" in general terms and conditions, but even the control of individually negotiated contracts.

**Objective interpretation of the parties' will?** This is completely new and it is obvious that this procedure has a paternalistic character. In this case, however, it is not attributable to the GDPR, but to the data protection supervisory authorities. The recklessness with which the supervisory authorities are willing to substitute their supposedly objective interpretation for the explicitly expressed will of the contracting parties confirms data protection law's tendency towards paternalism.

**Consequence:** The relationship that characterises the actions of public authorities now seems to filter through to contract law and direct civil law relations between citizens.

## Result

The GDPR contains numerous paternalistic elements that seek to protect citizens from the disclosure of data related to them. However, it is an imposed protection from which the citizen cannot escape in many cases.

**"Immature children":** The "paternal government (*imperium paternale*)", which *Immanuel Kant* deplored in 1793 because it makes citizens appear like "immature children" who "cannot distinguish what is truly useful or harmful to them" and which proves to be "the greatest despotism imaginable" (quoted from [Krönke](#)), is encountered again today in the form of the preventive state under data protection law [[Title C.11](#)].

**Echoes of "good policey":** In the 16th/17th century, the concept of "good policey" described a state of good order of the community as well as general welfare and, with the broad area of legally ordered coexistence, encompassed virtually the entire legal order, without making a distinction between public and private law. We seem to be approaching this state of affairs again in the scope of the GDPR.

**Against the paternalistic concept:** As a result, however, the GDPR risks incapacitating or patronising the citizen, which runs counter to the desired self-determination. The realisation that "well-intentioned" is often the opposite of "well-done" was ultimately one of the historical reasons why the paternalistic concept of "good policey" was finally abandoned in favour of more differentiated legal approaches.