Challenges of Digitalization - January 2020

// Joint Controllership

Reading time: 2-3 minutes

The ECJ recently passed three judgments on joint controllership under Art. 26 (1) GDPR (Facebook Fanpages - C-210/16; Jehovah's Witnesses - C-25/17 and Fashion ID - C-40/17). These judgements highlight and aim to sharpen this so far little deployed legal concept. In addition, the German supervisory authorities took a position on joint control in their DSK short paper No. 16. Controllers are well advised to review their procedures to identify joint controllerships and to take adequate measures to ensure compliance for related processing activities.

How to identify Joint Controllerships

Joint controllership requires two (or more) parties jointly determining the purposes and means of processing activities. In order to identify such joint control, one needs to assess the level of responsibility for each involved party and for any phase of a processing on a case-by-case basis and in accordance with the principles of ECJ case law. This may be a challenging undertaking as there may be cases where at first sight one would not tend to assume such joint control. This is due to the ECJ's broad interpretation of the legal concept of joint controllership in the interest of "**a high level of protection of fundamental freedoms and rights**" of affected data subjects.

Under these principles, to assume joint controllership, it is

- not mandatory that all parties have access to the affected personal data, and
- not necessary that the parties are equally involved in the processing of personal data.

Joint controllership may be assumed in case

- one party substantially controls and organises the data processing and the other con-tributes to it (only) by targeting the processing at a specific audience (ECJ Facebook Fanpages - C-210/16, para. 36),
- one party processes personal data and the other organises and coordinates its activi-ties without necessarily having access to the affected personal data (ECJ Jehovah's Witnesses - C-25/17, para. 63 et seq.) or
- one party embeds a plugin on his or her website, thus enabling processing of personal data by the other party (ECJ Fashion ID - C-40/17, para. 80).

What are the Consequences of Joint Controllership?

Joint controllers must

- ensure, within their own sphere of responsibility having in place a justification for the processing of personal data,
- conclude an agreement on joint controllership stipulating their roles and responsi-bili-ties in terms of data protection and in particular towards the data subjects and
- provide adequate information to the data subjects about their joint controllership and their respective roles.

Suggested Measures

Controllers should review their internal procedures for any activities possibly qualifying as joint controllership. There may be challenges along the road due to rather high level or too case specific guidance from ECJ case law. Therefore it appears prudent to also include more specific and hands-on guidance from the German supervisory authorities as provided in the DSK short paper No 16. According to which the following cases would qualify as joint con-trollership:

- clinical trials, involving multiple parties,
- common administration in terms of certain data processing (e.g. address data) within a group of entities,
- joint establishment of an infrastructure deployed for multiple parties to pursue their purposes, e.g. a jointly operated platform for travel organisation,
- recruitment services for several employers or
- joint operation of information or warning systems.

In the event of having identified a joint controllership, it is prudent to

- coordinate next steps with other involved (joint)controllers,
- implement an agreement on the joint controllership, and
- adequately inform the data subjects about the existence of a joint controllership and the essentials of the agreement on the joint controllership.

// Firm

Digitalization is a challenge for small and large companies alike. We are convinced that a flexible and specialized unit like **PLANIT** // LEGAL is best able to meet the needs of national and international clients.

PLANIT // LEGAL offers comprehensive advice on German and European **IT and data protection law**, both in the role of **external data protection officer**, **EU representative, legal advisor** and in a supporting role for legal, data protection and compliance departments.

We advise you on software licensing, IT procurement, e-commerce law, IT and data protection compliance as well as data protection and IT due diligence. Together with you, we develop solutions that fit your company. In doing so, we draft IT and data protection contracts, provide support for IT projects and represent your interests and rights in legal or regulatory disputes.

The lawyers of **PLANIT** // LEGAL have **many years of consulting experience** from IT and data protection departments of major international law firms, smaller units specialized in IT and data protection law, their work for data protection supervisory authorities and as company data protection officers.

PLANIT // LEGAL has a **strong network** and works closely together with colleagues from other jurisdictions or with other specialisations when necessary.

Contact

PLANIT // LEGAL
Jungfernstieg 1
20095 Hamburg
mail@planit.legal
+49 40609 44 190