# Social Media Account Holders Potentially Liable for GDPR Violations by Platform Operators

*June 27, 2018 – The TMCA*
by Ron Moscona and Tom Hutchinson

Social media is an important marketing channel for many organisations. It is also a convenient way by which marketers can learn about customers, through data collected when they use social media channels.


A recent case before the Court of Justice of the EU ("**CJEU**") highlights the potential liability of account holders for the data collection activities carried out by platform operators. Even though the case was decided on the basis of the old Directive, it may indicate the direction of things to come under GDPR and the risks arising to organisations and businesses that use social media to market themselves.

The case was brought by *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, the state data protection regulator in Schleswig-Holstein, one of the states of the German Federation. The regulator ("**ULD**") ordered a German educational services provider (*Wirtschaftsakademie Schleswig-Holstein GmbH* or "**Wirtschafts Academy**") to deactivate its social media account. According to the case report, the platform operator collected data from users using cookies that remained active for two years. The reference from the German court indicated that "neither Wirtschaftsakademie nor [the operator of the platform] notified [users of] the storage and functioning of the cookie or the subsequent processing of the data, at least during the material period for the main

## Related People

- Ron Moscona

## Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

proceedings".

The questions that were brought before the CJEU were: (a) whether it was appropriate for ULD to make an order against Wirtschafts Academy, given that the data collection was undertaken by the platform operator, not the account holder, and (b) whether ULD had jurisdiction over the platform operator, given that the data collection was undertaken by an entity in Ireland, not by a German undertaking.

The CJEU answered both questions positively. The decision points to a broad approach to questions of jurisdiction across territories and towards liability across different parties in the supply chain.

In regard to whether it was appropriate to issue an order against Wirtschafts Academy (effectively, whether the account holder was liable to the data collection activity) the question turned on whether it was to be treated as a "joint controller" of the data, alongside the platform operator.

Those already initiated in the language of GDPR would be familiar with the dichotomy between "data controllers" and "data processors". The distinction proved critical, for example, when proceedings were brought against Google Spain some years ago where a person asserted his 'right to be forgotten' seeking an order against Google to block links on its search engine to some old articles published about the individual. The EU court in that case rejected Google's defence that it was a 'mere processor' and therefore not required to comply with such requests. The CJEU held that Google was a data controller in relation to the listings produced by its search engine and as such is required by law to respect a person's request for the deletion of their data (if the request is based on valid grounds).

In the case of *Wirtschafts Academy*, the CJEU held that the account holder was "joint controller" of the data collected by the platform operator. The Court relied on the papers before it and found that the placing of cookies and collection of data from users was performed by the platform operator across its platform (making it a "controller" of the data). However, it explained, Wirtschafts Academy and others who set up their own pages on the social media platform give the operator "the opportunity to place cookies on the computer or other device of a person visiting its fan page" and further, according to the findings of the referring court, the administrator can define certain parameters when creating the pages "depending inter alia on the target audience and the objectives of managing and promoting its activities" which, the Court stated, "has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page". The Court also relied on the fact that the platform operator's offering included data analytics and that the account holder was able to request certain user data from the platform operator. Even though no investigation was carried out as to whether any such requests were in fact made by Wirtschafts Academy, the Court found the above sufficient to treat Wirtschafts Academy as a joint controller of the data collected from users.

The ruling suggests that a party can become exposed to liability under GDPR due to the processing of data by someone else, for instance in the context of service relationships

between them, at least where there is some degree of involvement with the data. Specifically, it establishes that in many cases account holders on social media services can potentially be held jointly liable to violations of GDPR by the platform operators in relation to data collected from users on the account holder's pages, for instance because their account settings impact on the way data is collected from users who visit their pages. It is difficult to predict in what other circumstances the court might reach this result, for example, if a customer is given access to data collected by a platform provider, could it be treated as a joint controller of the data? If so, would it be liable if the data was collected by the platform operator in violation of the law?

It is also unclear to what extent "joint controllers" are liable to each other's actions. The Data Protection Directive, which was the basis for the decision in the *Wirtschafts Academy* case, barely mentions the existence of joint controllers (the definition of "controller" in the Directive mentioned that there could be one controller or several joint controllers, but there were no provisions to allocate liabilities between them). Article 26 GDPR is much more detailed. It requires joint controllers to enter into an agreement between them in relation to their duties to data subjects and to advise data subjects of the essence of the agreement. It also provides that data subjects can exercise their legal rights against each of the joint controllers, regardless of the mutual arrangements between them. The decision in the *Wirtschafts Academy* case confirms that under the Directive an enforcement order could be addressed to a joint controller in relation to data collection activities by another controller. A similar approach could be taken under GDPR. This does not necessarily mean that a joint controller is *jointly* liable for violations of the law by the other.

The second issue considered by the CJEU concerned territorial jurisdiction. Although the question focused on issues of jurisdiction as between different EU member states, the broad approach adopted by the Court could reflect on its approach in the future to similar issues arising in relation to the international jurisdiction of GDPR.

The court in *Wirtschafts Academy* examined the provisions of Art. 4 of the Directive which defined the territorial jurisdiction of each EU Member State on issues of data protection. Each Member State under the Directive had jurisdiction over the data processing activities carried out "*in the context of the activities of an establishment*" in that Member State. The Court held that ULD, the German regulator, had jurisdiction over the matter because the data collection undertaken by an entity in Ireland had a sufficient nexus to the commercial activities of its affiliates in Germany (essentially, selling advertising to German customers).

GDPR defines its own international scope mainly by reference to the processing of the data being undertaken "*in the context of the activities of an establishment of the controller or the processor*" in the EU. The decision in *Wirtschafts Academy* suggests that even if the collection and processing of data are carried out entirely outside the EU, the activities could still be held to fall within the jurisdiction of GDPR if there is an EU undertaking that is sufficiently related to the activity. It should be borne in mind that GDPR jurisdiction can also be established on the basis that the data is processed in

connection with the offering of goods or services to individuals in the EU or collected in the course of monitoring their behaviour.