

March 21, 2018

EU Member State Courts Rule Against Facebook's WhatsApp in Decisions Providing Guidance on the Contours of Consent for Data Processing

WhatsApp has recently faced scrutiny by regulators about data processing consents it purported to obtain from users. Most recently, on March 15, the Spanish data protection authority ("AEDP") released a decision imposing the maximum fine of €300,000 against Facebook and WhatsApp for processing personal data without consent. The AEDP found that WhatsApp did not receive valid consent to process users' data, since their continued use of WhatsApp was conditioned on providing such consent and was therefore not freely given. The AEDP also concluded that WhatsApp failed to clearly present information regarding the purposes for processing user data and how such data would be shared. Additionally, on March 14, WhatsApp pledged to cease sharing its United Kingdom users' data with Facebook until the General Data Protection Regulation ("GDPR") takes effect, after the UK's data protection authority, the Information Commissioner's Office ("ICO") concluded WhatsApp did not have a lawful basis of processing to share such user data with its parent company. The ICO also found that WhatsApp failed to adequately inform users about how their data was to be shared.

These decisions follow similar holdings in Germany, the latest a March 1 decision from the Higher Administrative Court of Hamburg (the "Court"). Although the decision was made under German law, it provides helpful guidance on the contours of effective consent in a wider European privacy law context, including under the GDPR. Because of its discussion of the notices required to obtain effective consent, this Alert discusses the Court's decision in greater detail.

Background

The German Federal Data Protection Act ("BDSG") permits the collection, processing and use of personal data only if a data controller meets certain requirements (the details of which are not relevant here) or if the data subject has consented. Under the BDSG, "effective consent" must be based on a data subject's "free decision." Among other things, the data processors must inform data subjects of "the purpose of collection, processing or use and, insofar as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent." Additionally, the law stipulates that "[i]f consent is to be given together with other written declarations, it shall be made distinguishable in its appearance." The GDPR, which comes into effect on May 25 of this year, contains similar requirements. Controllers may process data only on the basis of at least one of the conditions enumerated in Article 6(1), one of which is obtaining user consent. Consent is defined in Article 4(11) as any "freely given, specific, informed and unambiguous indication of the data subject's wishes."

In September 2016, the Hamburg Data Protection Regulator (the "Regulator") barred Facebook from collecting and storing personal data of German WhatsApp users who had not given the consent required under Section 4a of the BDSG. Facebook challenged this decision before the Regulator and subsequently applied for interim measures before the Hamburg Administrative Court. Due to the nature of the proceedings, the court conducted a summary examination of the case and largely sided with the Regulator in its order on April 24, 2017. Facebook then brought the case before the Higher Administrative Court of Hamburg. Again, due to the nature of the proceedings, the Court conducted a summary examination of the case, mostly agreeing with the lower court, and ultimately, the Regulator. In its decision on WhatsApp, the Court found that Facebook likely violated BDSG provisions by collecting and

storing the personal data of German users of its WhatsApp subsidiary. The Court concluded that Facebook's consent provisions in notices to its German WhatsApp users about terms of use updates may be insufficient and in violation of the German privacy law. The decision contains guidance that is relevant (though not binding) for data controllers.

WhatsApp's Failure to Seek Effective Consent

In Germany, the Higher Administrative Court of Hamburg issued a decision carefully analyzing the disclosures made by WhatsApp. WhatsApp had required users to accept its privacy guidelines, which included consents to the processing of user information, in order to continue using the service. The Court found that WhatsApp did not provide its users with the opportunity to give effective consent to data processing as required under Section 4a of the BDSG. The Court explained that such requirements ensure that data subjects are not agreeing to items "hidden in the small print"—data subjects must understand the circumstances under which they consent to the processing of their data and what the consequences of their decisions are.

In Facebook's case, the Court found that WhatsApp fell short on providing effective consent to data processing in the notice it provided to users regarding terms of use and data privacy guidelines updates, for several reasons:

- It was not clear for average users that by clicking the hyperlink to "agree" to WhatsApp's updated terms of use and data privacy guidelines that users would also be consenting to the processing of their data. The Court found it misleading that the text¹ before and after this hyperlink did not itself refer to data processing. Rather, the surrounding language communicated that WhatsApp's data protection guidelines were being updated and referred users to those guidelines. Users were asked to agree to the guidelines to continue using WhatsApp but were not told that by agreeing they were consenting to the processing of their data.
- When seeking user consent, WhatsApp explained that it had updated its terms of use and "data protection guidelines." To the Court, the language was misleading because it suggested the update was designed to "protect" users' data—when in fact, WhatsApp was seeking consent to process their data.
- The link to "opt out" of agreeing to the update notice was unclear and not made distinguishable, and the notice's statement that "independent of this setting [i.e., opting out], your chats and phone numbers are not shared on Facebook" was misleading to users.

In light of this guidance, companies relying on consent as a basis for processing should consider whether they are providing adequate notice to users to receive effective consent. Considerations may include whether the text immediately surrounding any consent button or link itself alerts users to expected processing activities and whether opt-outs are sufficiently clear and distinguishable from other text or features.

No Back-Up Bases for Processing after Seeking User Consent

One additional question the Court addressed of interest to companies seeking to comply with the European privacy regime is whether, even if consent is subsequently invalidated, Facebook could rely on another basis for processing. As discussed, under the BDSG (and the impending GDPR), each data processing activity (including data collection and sharing) must be based on the consent of the data subject or some other legal basis. In the Court's assessment, if a company's bases for processing user data for a particular purpose include both consent and processing "prescribed by a legal provision," and the consent later turns out to be invalid, it is "at the very least doubtful" that a company could rely on its other claimed legal basis for the same processing activity. The Court reasoned that the act of seeking data subjects' consent will lead them to believe they have the power and ability to avoid the respective processing of their data. That analysis appears in line with guidance issued by the Article 29 Data Protection Working Party for the

¹ The full text of the surrounding language read: "WhatsApp is updating its terms of use and its data protection guideline in order to account for new functions, like WhatsApp Call. Read our terms of use and data protection guidelines and learn more about your choices. Please agree to the terms of use and the data protection guideline by 25 September 2016 in order to continue using WhatsApp."

GDPR, which has explained that a controller cannot fall back on another basis of processing for a particular purpose if the consent it sought for that same purpose is later determined to be invalid.