Doing Business in Europe? Social Media Prosecution in Germany Flags Data Consent Problem for All Businesses

by Rafi Azim-Khan and Steven P. Farmer

Do you transfer personal data from Europe to the US? Do you use cookies on a website which is aimed at European customers? Do you send marketing emails to Europe? Do you otherwise "process" data in Europe? Do you really *have consent to process personal data? If any of these questions strike a chord with you, then you should certainly note recent trends in the EU regarding the concept of "consent," not least the news from Germany that Facebook is to be prosecuted (and potentially fined up to $400,000) over its facial recognition software feature and for failure to properly obtain consents.*

This issue of what constitutes proper consent, or not, has been coming to the boil in 2011.

A recent Opinion published by the Article 29 Working Party (the grouping of data protection authorities from each EU state - the "Working Party"), looked again at the concept of "consent," which, subject to certain exceptions, is required from individuals before such activities are carried out. Adopted 13 July 2011, it was aimed to provide a thorough analysis on the concept of consent as currently used in the European Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC.

Germany's Hamburg Data Protection Authority (DPA) announcement that it is now to start proceedings against Facebook over its facial recognition feature and photo tagging has further highlighted what a problem the issue of consent can be in the EU. The DPA, like many other EU enforcers, has been losing patience with companies who don't seem willing to comply with the black letter requirements, particularly around consent, and what many have "got away with" in the past will now likely generate trouble and possible exposure to increasingly large fines. Dismissing Facebook arguments that a checkbox element amounted to compliance, the DPA is reported as saying further negotiation is "pointless" and will now look to enforce compliance with fines of up to 300,000 euro (over $400,000).

Just to top it all, we have, of course, also had confirmation this past week that proposals to overhaul the DP Directive itself should be forthcoming early in 2012.

This alert will look at the complex issue of consent and see if the recent Opinion has at least managed to shed some light.

Consent clarified?

One of the Opinion's main aims is to clarify the existing legal requirements surrounding the obtaining of consent, given this is such a key issue which crops up time and again.

The Working Party's Opinion will be persuasive in the eyes of the various European privacy regulators when making enforcement decisions, making it very worthwhile for companies, including US companies, doing business in Europe to pay close attention to its detail.

The requirement for consent

In a nutshell, under the Data Protection Directive, personal data can only be "processed" (i.e., collected, stored, amended, transferred, deleted etc) in Europe in fairly limited circumstances. One legal basis that gives a data controller the right to process personal data, however, is "unambiguous consent of the data subject."

Further, the processing of "sensitive" personal data (medical, religious, etc.) requires "explicit consent" (unless some narrow legal grounds apply).

The Data Protection Directive goes on to define consent as "any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

The e-Privacy Directive also introduces the notion of consent, requiring the "consent" of individuals, for example, before they are sent electronic marketing communications such as emails, or before cookies are placed on their hard drives.

It can be seen, therefore, that understanding the varying approaches to the issue of consent is critical. The Opinion seeks to clarify how companies can obtain consent correctly to avoid a number of pitfalls which surround this issue. In particular, it explores in detail what "any … indication of his wishes," "freely given," "specific," "informed," "unambiguous" and "explicit" mean in practice.

"Any ... indication of his wishes"

The Working Party considers that an "indication" is "any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes and to be understandable by the data controller."

In other words, consent cannot be inferred from a lack of action. This would appear, therefore, to be the death-knell in terms of the use of pre-ticked boxes which are a common way in which companies attempt to obtain consent.

"Freely given"

"Freely given" consent means that "there must be no risk of deception, intimidation or significant negative consequences for the data subject if he/she does not consent," says the Working Party.

It follows, therefore, that it would not be possible for a US company to say to an employee in Europe that he or she will consent to his or her data being transferred to the US otherwise he or she will not get paid (consent to a transfer being one of the ways which an extra-European transfer of data can legitimately be made). Some other workaround would be required to ensure the consent was valid and/or the transfer could be made.

"Specific"

The Working Party goes on to consider that "blanket consent without determination of the exact purposes does not meet the threshold" in the context of the meaning of "specific" consent.

When seeking consent, therefore, rather than inserting the processing information in the general conditions of a contract, for example, specific consent clauses separated from the general terms and conditions should be considered in order to avoid falling short on this point.

"Informed"

Consent is "informed," when the information provided is sufficient to guarantee that individuals can make well-informed decisions about the processing of their personal data.

The Working Party considers that, first, the way that information is given must ensure the use of appropriate language so that individuals understand what they are consenting to and for what purposes. So for instance, the use of overly complicated legal or technical jargon would not meet legal requirements.

Second, the information provided to individuals should be clear and sufficiently conspicuous so that users cannot overlook it. It should not be "hidden" on a website, for example.

"Unambiguous consent"

According to the Working Party, "unambiguous consent calls for the use of mechanisms to obtain consent that leaves no doubt as to the individual's intention to provide consent."

In practical terms, this requirement obliges companies to adopt mechanisms to seek a "permanent" record of the consent such as an email record.

"Explicit consent"

The Working Party considers that "explicit" consent is similar to "unambiguous" consent and it means "an active response, oral or in writing, whereby the individual expresses his/her wish to have his/her data processed for certain purposes."

It is considered, as above, that explicit consent cannot be obtained by the presence of a pre-ticked box, for example, and that consent should be recordable.

So what does all this mean for US companies (and those located elsewhere) doing business in Europe?

It is crucial that US companies (and those located elsewhere) first consider fully whether their activities in Europe with regard to the processing of personal data will require the consent of individuals before data is processed.

Consent will generally be required for a very wide range of activities, for example, when placing cookies on potential customers' hard-drives in Europe, transferring names and other details to the US from Europe or selling a mailing list to a third party.

Companies should then bear the following in mind where consent is required for activities covered by the Data Protection Directive or the e-Privacy Directive:

Consent must be provided *before* the processing of personal data starts.

Consent *cannot be inferred from a lack of action* – it is far safer to obtain a signature, request that a box be ticked, etc.

No negative consequences must be attached to a failure to give consent.

Beware of "blanket" consents – it is safer to separate the different consents required in any given scenario (e.g., pop-up boxes to seek consent).

Keep the language clear and simple when seeking consent – avoid legal jargon.

Keep a record of all consents obtained.

Individuals who have consented should be provided with a method by which they can withdraw their consent.

As stated, whilst the Working Party Opinion is not law per se, it will be taken seriously into consideration by the national regulators in Europe who do have teeth to bite those who trip over the rules on consent or those who blatantly flout them.

US companies, and those doing business elsewhere, are urgently encouraged, therefore, to audit their data processing activities in Europe and to regularly monitor these activities to ensure they do not become a victim of increasingly tough sanctions for breach of European data protection laws relating to consent.

Aside from the freshly announced action in Germany against Facebook, we also have a fairly new enforcer in the UK who has recently been given significantly stronger powers, including the power to issue fines over $750,000 on the spot, per offence. Conducting a fresh review of your data processing and transfer activity has never been more timely or well-advised.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors of this alert.

Rafi Azim-Khan (bio)
London
+44.20.7847.9519
rafi.azimkhan@pillsburylaw.com

Steven P. Farmer (bio)
London
+44.20.7847.9526
steven.farmer@pillsburylaw.com