EU Court of Justice likely to continue firm line on data protection and ePrivacy in 2019

The entry into force of the General Data Protection Regulation (GDPR) on 25 May made 2018 a landmark year for data protection. In its wake, companies have finalised their GDPR compliance efforts, the tide of updated privacy policies and renewed consent requests has receded, and data protection authorities in member states have been slowly settling into their new enforcement roles.

Contrary to some predictions, the first six months of GDPR’s application did not yield unprecedented fines (which can be as high as 4% of global annual net turnover of an undertaking), since most enforcement actions still covered pre-GDPR violations. But in 2019, the European privacy novel will start a new chapter. Fines will rise. In addition, the EU’s highest court (CJEU) is expected to shed light on several core elements of the GDPR and the ePrivacy framework, such as requirements for consent online, mass surveillance on national security grounds, and the validity of standard contractual clauses widely used as legal grounds for international transfers of personal data. In a recent speech, President Koen Lenaerts of the Court of Justice of the European Union (CJEU) emphasised that many data protection cases are pending at the CJEU. We expect several of those cases to be decided in the coming year, and they undoubtedly will have a significant impact on companies’ data governance and business models.

“Cookies” consent

The “Planet49” case will shed light on whether user’s online “cookie” consent provided by way of unselecting a pre-checked checkbox (in other words, opt-out) constitutes valid consent under the GDPR and the ePrivacy rules. The CJEU will also have to clarify the type of information an electronic communications service provider must give users before the latter can consent. An oral hearing took place in November 2018, and the Advocate General’s opinion is due in late February 2019. After that, the Grand Chamber of the court will rule on the case, which underscores how important the outcome is.

The issue of online “cookie” consent has been a contentious issue in the legislative process of the EU’s draft ePrivacy Regulation, the GDPR’s counterpart for electronic communications. The legislative progress on the draft ePrivacy Regulation is currently stalled and will not continue until after European Parliament elections take place in May 2019. We expect the CJEU’s interpretation to have a decisive influence on how this issue.
will be resolved in the regulation.

**Bulk sharing of electronic communications data with authorities**

Another important case on ePrivacy currently pending at the CJEU concerns the sharing of bulk electronic communications with security and intelligence services by electronic communications providers. The main issues to be decided are whether the retention and sharing of these communications with governmental services falls under the EU ePrivacy rules and, if so, when and under which conditions these communications can be shared. Since consensus on this has yet to be reached in the draft ePrivacy Regulation, the CJEU’s judgment is likely to shape the wording of the regulation on this point. Moreover, the CJEU will signal the extent to which it sees a role for itself in national security matters, in addition to the European Court of Human Rights. Lately, the CJEU has adopted a strict position on privacy.

**The notion and mutual responsibilities of joint controllers**

The Fashion ID case will add to several CJEU cases tailoring the interpretation of a “joint controller”, as introduced by the GDPR, in specific contexts. This case will impact all companies using social plug-ins on their websites. In the opinion delivered on 19 December 2018, Advocate General Bobek suggests that a website operator which embedded a Facebook “Like” button plug-in, qualifies as a joint controller together with Facebook. By integrating the plug-in into its website, the website operator co-determines the parameters of personal data collection by Facebook which, in the opinion of AG, is sufficient to pass the low threshold of a “data controller”.

This approach is in line with the broad interpretation of this term adopted by the CJEU in two 2018 cases, Wirtschaftsakademie Schleswig-Holstein and Jehovah todistajat. In the first case, the CJEU recognised a Facebook fan page administrator as joint controller on par with Facebook. In the second case, members of a religious community proselytising on a door-to-door basis were considered joint controllers on par with the religious community itself. In both cases, the CJEU ruled that access to personal data is not a prerequisite for qualifying as a joint controller. In this particular case and unlike prior cases, the AG outlined how joint controllers should share mutual responsibilities: namely, that consent for the collection of personal data by means of a Facebook “like” plug-in, where required, should be obtained by the website operator.

**Personal data transfers outside the European Economic Area**

Finally, in 2019 we expect the CJEU to decide on the validity of Standard Contractual Clauses (SCCs) raised in Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, as referred to the CJEU by the Irish High Court. SCCs underpin a substantial portion of personal data transfers to countries outside the European Economic Area (the EU + Norway, Iceland and Lichtenstein) that do not provide an adequate level of personal data protection. In late January 2019, the Irish Supreme Court will hear Facebook’s appeal, where Facebook seeks to reverse the referring of questions to the CJEU or the
altering of questions formulated by the referring court. The outcome of this case will affect the compliance costs of companies whose business involves cross-border data flows.

**Looking ahead**

In recent years, the CJEU has affirmed its role as the EU’s human rights court. We expect the CJEU to strictly interpret these pending issues in light of the EU Charter of Fundamental Rights, re-affirming the strict interpretation of the Charter and its new fundamental right to data protection. In the meantime, we will monitor the progress of these cases and keep you informed on important developments.