CJEU Clarifies When Supervisory Authorities Can Derogate from One-Stop-Shop

On 15 June 2021, the Court of Justice of the European Union (***CJEU***) handed down a judgment in which it ruled that, under certain circumstances, a national supervisory authority may exercise its power to bring any alleged infringement of General Data Protection Regulation (EU) 2016/679 (the ***GDPR***) to a court in a Member State, even though that authority is not the lead supervisory authority (***LSA***) with regard to such processing. The judgment provides important clarifications on the functioning of the "one-stop shop" mechanism under the GDPR and the possibility for national supervisory authorities to bring court proceedings outside this mechanism.

Background

The question arose in proceedings initiated by the President of the former Belgian Privacy Commission in September 2015 against Facebook before the Dutch-speaking Court of First Instance of Brussels (*Nederlandstalige Rechtbank van eerste aanleg te Brussel / Tribunal de première instance néerlandophone de Bruxelles*; the ***Court of First Instance***). Facebook Ireland, Facebook Inc. and Facebook Belgium (the ***Facebook group***) allegedly infringed Belgian data protection laws, including by collecting and using information on the browsing behaviour of Belgian internet users, whether or not they were Facebook account holders, by means of various technologies, such as cookies, social plug-ins or pixels.

On 16 February 2018, the Court of First Instance ruled that Facebook's cookies (and similar technologies, such as pixels) infringed Belgian data protection laws. Moreover, it held that Facebook had failed to adequately inform Belgian internet users about the collection and use of the information concerned (our Client Alert on this ruling at first instance can be read here). The Court of First Instance accepted territorial jurisdiction over the Facebook group, even though Facebook's main establishment is located in another Member State, and held that it was necessary for the Belgian Privacy Commission to be able to bring a claim before the national court in order to have effective supervisory powers. The Facebook group appealed the decision to the Brussels Court of Appeal (*Hof van Beroep te Brussel / Cour d'Appel de Bruxelles*; the ***Court of Appeal***). The Belgian Data Protection Authority (***DPA***) acts as the legal successor of the President of the former Privacy Commission in the appeal procedure.

The CJEU's judgment: When can a supervisory authority that is not the LSA initiate legal proceedings against a controller for alleged infringements of the GDPR?

The preliminary question raised by the Court of Appeal concerns the "one-stop shop" mechanism, introduced by the GDPR. Under this mechanism, the supervisory authority of the location where a company has its EU headquarters (i.e., the lead supervisory authority or ***LSA***) is competent to decide in matters relating to cross-border processing of personal data (Article 56.1 GDPR). The referring court sought to know whether and to what extent the Belgian DPA could have competence in this cross-border case in which Facebook Ireland has been identified as the controller of the data concerned. In the case at hand, the Irish DPA is the LSA and the competent authority to bring injunction proceedings subject to review by the Irish courts.

In its judgment, the CJEU points out that the competence of supervisory authorities to adopt decisions on cross-border processing activities must be exercised with due regard to the cooperation and consistency

procedures provided for by the GDPR. In general, the "one-stop shop" mechanism requires close, sincere and effective cooperation between supervisory authorities, in order to ensure consistent and homogeneous protection of the data protection rules. The mechanism guarantees the competence of the LSA for the adoption of a decision finding that a cross-border processing activity infringes the GDPR. The competence of the other supervisory authorities concerned to adopt such a decision, even provisionally, is only allowed in exceptional cases. However, in the context of a "*sincere and effective cooperation between supervisory authorities*", the LSA cannot ignore the views of the other supervisory authorities. Any relevant and reasoned objection made by one of the other supervisory authorities has the effect of "blocking", at least temporarily, the adoption of the draft decision of the LSA. The exercise of this power by a supervisory authority that is not the LSA is also in line with Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, which guarantee data subjects the right to the protection of their personal data and the right to an effective remedy.

Second, for a supervisory authority that is not the LSA to exercise its power to initiate or engage in legal proceedings with regard to cross-border processing, it is not a prerequisite that the controller in question has a main establishment or other establishment on the territory of that Member State.

Third, this supervisory authority can exercise its power both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power. The CJEU adds that the exercise of this power presupposes that the GDPR is applicable. In the case at hand, since the activities of the establishment of the Facebook group located in Belgium are inextricably linked to the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the EU, that processing is carried out "in the context of the activities of an establishment of the controller" and, therefore, does fall within the scope of the GDPR.

Fourth, the CJEU considers that the proceedings were initiated before the entry into application of the GDPR and continued after the GDPR had come into force. In such a case, the CJEU holds that the action may be continued, under EU law, on the basis of the provisions of the former Data Protection Directive 95/46/EC. In addition, that action may be brought by that authority with respect to infringements committed *after* the entry into force of the GDPR, provided that: (i) the authority is permitted under the GDPR to adopt a decision notwithstanding the "one-stop-shop mechanism" (e.g., in case of a purely local breach or to adopt an urgent, provisional measure) and (ii) the cooperation and consistency procedures provided for by the GDPR must be respected.

Finally, the CJEU recognises the direct effect of the provision of the GDPR under which each Member State is to provide by law that its supervisory authority is to have the power to bring infringements of the GDPR to the attention of the judicial authorities and, where appropriate, to initiate or otherwise engage in legal proceedings. Consequently, such an authority may rely on that provision in order to bring or continue a legal action against private parties, even where it has not been specifically implemented in the legislation of the Member State concerned.

The full judgment of the CJEU is available here.