



CLERKIN LYNCH LLP

Recent ECJ Decision on cross border data processing – Potential for multiple exposures?

Mark Browne

Partner and Head of Asset Management
and Funds at Clerkin Lynch LLP

8/10/2021

Recent ECJ Decision on cross border data processing:

Potential for multiple exposures

The GDPR's 'one stop shop' (the 'OSS') mechanism was created to allow companies which have establishments in various Member States in the EU to liaise solely with the data protection authority in which it has its main establishment. This data protection authority is known as the 'lead supervisory authority' ('LSA') and is responsible for dealing with all cross-border data processing which that company engages in across the EU.

On 15 June 2021, the Court of Justice of the European Union (the "CJEU") released its judgment in the Facebook Ireland & others v the Belgian Data Protection Authority Case C 645/19. In this judgment, the ECJ analysed the application of the OSS mechanism and the circumstance in which a national supervisory authority, which is not considered the LSA, can investigate alleged infringements and initiate legal proceedings.

Summary of Judgment

The Brussels Court of Appeal made a request for a preliminary ruling under Article 267 TFEU and referred six questions to the Court. The request was made in proceedings between Facebook Ireland Ltd, Facebook Inc. and Facebook Belgium BVBA and the Belgian Data Protection Authority ('the DPA'). In these proceedings, a judgment was sought against Facebook Ireland, Facebook Inc., and Facebook Belgium before the Court of First Instance in Belgium and sought to bring an end to Facebook's processing of user's personal data within Belgium through the use of cookies, social plug-ins and pixels.

In the view of the referring court and with respect to facts subsequent to 25 May 2018, the main question which arose was whether the DPA in Belgium could bring proceedings against Facebook Belgium notwithstanding the fact that in accordance with Article 56 of Regulation 2016/679 (the "Regulation"), the Irish Data Protection Commissioner was the competent body to bring such proceedings.

The first question referred to the Court was seeking to ascertain whether Article 55 (1), Articles 56-58 and Articles 60-66 of the Regulation, read together with the articles 7,8 and 47 of the Charter, must be interpreted as meaning that a supervisory authority of a Member State has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State, and if necessary, to initiate or engage in legal proceedings and may exercise that power with respect to cross border data processing of that data even though it is not the 'lead supervisory authority'. The Court held that, in the event of cross border data processing, the supervisory authority has the power to bring any alleged infringement of the Regulation to the attention of the court of that Member State and can initiate and engage in legal proceedings even though it is not the LSA.

The second question referred to the Court sought to ascertain whether Article 58 (5) of the Regulation must be interpreted as meaning that, in the event of cross border data processing, it is a prerequisite for the exercise of the power of a supervisory authority of a Member State (other than the LSA) to initiate or engage in legal proceedings, that the controller, against whom such proceedings are brought against, has a 'main establishment' or another establishment in that Member State.

The court concluded that in the event of cross border data processing, it is not a prerequisite for the exercise of the power of the supervisory authority of a Member State

(other than the LSA) the company against whom proceedings are brought has its main establishment or another establishment in that Member State.

The third question referred to the court sought to ascertain whether article 58 (5) of the Regulation must be interpreted as meaning that, in the event of cross border data processing, it is a prerequisite of the exercise by a supervisory authority (other than the LSA) of the power to bring any alleged infringement of that regulation to the attention of the court of that Member State , and where necessary initiate or engage in legal proceedings, that the supervisory authority directs its legal proceedings against a main establishment of the controller or against the establishment that is located in this own Member State.

The court concluded that the article must be interpreted as meaning that the power of the supervisory authority to bring any alleged infringement of the Regulation to the attention of a court of that Member State and where appropriate initiate or engage in legal proceedings, may be exercised with respect to the both the main establishment and the controller which is located in that authority's own Member State provided that the object of the legal proceedings is processing of data carried out in the context of the activities of that establishment and that authority is competent to exercise that power, in accordance with the answer to the first question referred to the court.

The fourth question referred to the court sought to ascertain whether article 58 (5) of the Regulation must be interpreted as meaning that where a supervisory authority of a Member state (that is not a LSA) has brought proceedings concerning cross border transfer before the commencement of the Regulation, this will affect the conditions governing whether a Member states' supervisory authority may exercise the power to initiate or engage in legal proceedings conferred on it under the Regulation.

The court concluded that where the supervisory authority (who is not a LSA) has brought proceedings which involve cross border processing of personal data prior to the commencement of the Regulation, that action may be continued on the provisions of Directive 95/46 which remains applicable up to the 25 May 2018, the date when the directive was repealed.

The fifth question, which was contingent on receiving an affirmative answer to the first question, sought to ascertain that Article 58 (5) must be interpreted as meaning that the provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue legal proceedings against private parties even when that provision has not been implemented in the legislation of the Member State concerned.

The court concluded that the provision must be interpreted as meaning that it does have direct effect with the result that a national supervisory authority may rely upon the provision in order to bring or continue legal proceedings against private parties, even where it has not been implemented in legislation of the Member State concerned.

The court concluded that the final question was a hypothetical problem which had no relevance to the facts of the case and therefore, the court declared it inadmissible.

Impact of the ECJ's decision (cont):

This judgment makes it clear that in certain circumstances, national supervisory authorities can handle data privacy complaints and initiate legal proceedings even where that national supervisory authority is not considered the LSA, and the company does not have its main establishment in that Member State.

It is unclear what the full extent this ruling will have on the OSS mechanism as yet, but it has the potential to undermine this mechanism and diminish the certainty which it sought to provide to companies which operate across the EU. It will be interesting to see how this

Impact of the ECJ's decision:

judgment will be interpreted and how it will affect the operation of the OSS mechanism. In particular, companies will need to consider whether opening a branch or physical operation in another Member State may result in additional risk and expose them to potentially undue burdens being placed on them as a result of this judgment.

Data Protection in Clerkin Lynch

Clerkin Lynch has extensive experience advising clients on data protection issues and dealing with the Data Protection Commissioner. Following the introduction of Regulation (EU) 2016/679, The General Data Protection Regulation (GDPR) a range of new data protection requirements and potential risks is applicable upon businesses and those controlling or processing personal data. Clerkin Lynch acts not only for businesses in relation to their own data protection policies and obligations but also acts for individuals who believe that their rights have been infringed as a result of a data breach or other related matters.

Authors



Mark Browne
Partner
Head of Asset Management
and Funds
Email: markbrowne@clerkinlynch.com
Phone: +353 1 611 4400



Eileen Woods
Trainee Solicitor