European Court Ruling on Joint Controllers and Website Social Plug-ins (Facebook “Like” button)

Date : August 22, 2019

Introduction

Generally-speaking the issue of joint controllership of personal data is becoming more and more prominent. Under this concept, where two or more data controllers jointly determine the purposes and means of data processing they are considered as joint controllers (as opposed to being e.g. in a controller-processor relationship), which has particular consequences for data protection responsibilities, obligations and liability.

The European Court of Justice recently made an important ruling about joint personal data controllership and website operators using website social plug-ins (tools consisting of pieces of software code that website owners can use on their websites provided for user social experience), which in this particular case concerned the Facebook “Like” button. This judgement comes in a recent line of European Court judgements about joint controllers, which we have previously written about here https://www.corderycompliance.com/european-court-ruling-in-jw-data-protection-case-2-2/ and here https://www.corderycompliance.com/client-alert-european-court-facebook-fan-page-ruling/.

This article sets out the highlights and takeaways of the judgement.

What is this case about?

In brief, the German online clothing retailer Fashion ID embedded the Facebook “Like” button on its website through which personal data, i.e. IP addresses, along with browser technical data, of individuals visiting the Fashion ID website was automatically sent to Facebook Ireland (the location of the European HQ) – this occurred irrespective of whether or not those visiting the Fashion ID website had Facebook accounts or had actually clicked the button or not; users did not have the possibility of stopping the transmission of their data.

The German consumer protection organisation “Verbraucherzentrale NRW” was concerned about the lack of consent and information disclosure with regard to the transmission of personal data and brought legal action seeking an injunction against Fashion ID to stop the practice in question, on the basis that the use of the Facebook “Like” button infringed the then existing EU data protection rules. The case was then referred by a German court to the European Court of Justice for a preliminary ruling on the interpretation of data protection rules concerning a number of issues.

What did the court rule?

The European Court ruled that Fashion ID and Facebook Ireland were joint controllers with respect to the collection and disclosure by transmission of the website users’ personal data to Facebook Ireland.

According to the court, “[…] Fashion ID appears to have embedded on its website the Facebook ‘Like’ button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook. Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin”.

Further, “[a]s to the purposes of those operations involving the processing of personal data, it appears that Fashion ID’s embedding of the Facebook ‘Like’ button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to

benefit from the commercial advantage consisting in increased publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID."

But the court also ruled that "[…] it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations […]". Presumably this logic would also apply to situations (i.e. in other social plugin scenarios) involving prior personal data processing.

In the context of the collection and transmission of personal data website by means of the social plugin in question, the issue of the lawful basis of processing was also examined by the court. Where "legitimate interests" was being considered (as opposed to consent) as the lawful basis, as regards exactly whose "legitimate interests" should be taken into account when relying on "legitimate interests" (in the context in question), the court ruled that each of those [joint] controllers should pursue a legitimate interest […] through those processing operations in order for those operations to be justified in respect of each of them".

Finally, the court also ruled that with regard to who is responsible for data protection consent and information disclosure requirements: "[…] in a situation […] in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, […] consent […] must be obtained by that operator only with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means. In addition, […], in such a situation, the duty to inform […] is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means."

The judgement can be found here http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0040&lang1=en&type=TXT&ancre=.

Takeaways

Although this judgement was decided with respect to the previous EU data protection regime it is likely that the same findings and considerations would be made with regard to the EU General Data Protection Regulation (GDPR); this specifically deals with joint controllers under Article 26.

The court's judgement is in line with a series of rulings where it has given a wide interpretation to the notion of joint controllers.

Probably the most significant consequence of this ruling is that it increases liability risk for organisations operating websites when they integrate social plug-ins and third-party content. In practical terms key takeaways are as follows:

- Organisations operating websites using social plugins (including e.g. Twitter and LinkedIn) should have a joint controller agreement in place with the social plugin service provider that sets out the parties' respective responsibilities, obligations and liabilities – organisations should also do due diligence on the social network as regards their compliance with data protection requirements;
- Data protection information and disclosure requirements will need to be complied with, essentially through updating the (external) privacy policy to inform website visitors about the processing of their data in relation to the plugins and about the joint controller agreement with the plugin provider; and,
- The appropriate lawful basis will need to be determined and applied as regards processing personal data in relation to the plugin – consent is likely to be the more appropriate basis (as determined on a case by case basis) to be obtained from individuals visiting the website, using an appropriate consent mechanism.

Finally, think about other instances of matters that you're handling with organisations who you're working with

where you might be considered as a joint controller.

Compliance failure in this area could lead to regulator enforcement and subsequent fines and possible compensation claims by aggrieved individuals.

For other articles that we have written about data protection compliance please see here: https://www.corderycompliance.com/category/data-protection-privacy/

For more information on GDPR see details of Cordery GDPR Navigator here www.bit.ly/gdprnav.

Cordery's Breach Navigator can help organisations respond to a breach and assess its consequences. There are more details here https://www.corderycompliance.com/solutions/breach-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com