Joint controller relationships — more prevalent than previously thought?

Duc Tran, Senior Associate, and Laura Adde, Associate, at Herbert Smith Freehills LLP, examine the concept of joint controllership in light of recent case law and existing (albeit limited) guidance

Since the General Data Protection Regulation ('GDPR') came into force, there has been a steady trickle of judgments throughout Europe on many aspects of data protection and privacy. One area of the GDPR which until recently, had not been tested by the courts was the concept of joint controllership. However, this area of GDPR compliance has now been brought to the fore, as the Court of Justice of the EU ('CJEU') handed down judgment on the German 'Fashion ID' joint controller case (C-40/17). The judgment could mean that many organisations previously not designated joint controllers could now be. This is because the judgment expands the meaning of 'joint controller' as it was previously understood.

Since the GDPR has been in effect, organisations have tended to characterise their data relationships with other parties as either controller-processor relationships, or independent controller -controller relationships, avoiding the joint controller construct either due to the apparent specificity of the legislation, or concerns around the regulatory consequences of being in a joint controller relationship (joint and several liability, for example).

The Fashion ID case suggests that in fact, joint controller relationships may be far more prevalent than previously thought. This article seeks to clarify the implications of this new decision and, by reference to existing (albeit limited) guidance, explain what it could mean for organisations in practice.

The Fashion ID case

Like many other organisations, German clothing retailer Fashion ID embedded the well-known Facebook 'Like' plugin on its website, enabling customers to 'like' Fashion ID on Facebook at the click of a button.

Where website operators embed third party plugins on their website, the third party's content is displayed on the website. In order to do this, plugins transmit website visitor data (such as IP addresses, which are considered 'online identifiers' and therefore personal data) to the servers of the third party, in order to request content from the third party in the correct format for the visitor's browser. The website operator has no control over what data the visitor's browser transmits, nor over what the third party does with that data.

In this case, when visitors accessed the Fashion ID website, their personal data were transmitted to Facebook via the plugin, regardless of whether the visitor clicked on the 'Like' button or whether they were a Facebook user. The CJEU held that website operators that embed third party plugins of this type (i.e. Fashion ID) can be considered joint controllers with the third party (i.e. Facebook) within the meaning of the GDPR, although the website operator's liability will be limited to the extent to which the operator determines the purposes and means of processing personal data (i.e. the collection and disclosure via transmission). The website operator will also be responsible for providing fair processing information and obtaining any necessary consents to the extent to which it determines the purposes and means of processing.

Whilst organisations will continue to use such plugins following this judgment, it raises significant questions about what does, and does not, constitute a joint controller relationship.

Defining joint controller relationships

Article 26 of the GDPR states that 'where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers'. This is not entirely dissimilar to the position under the previous legislation, which provided that where two parties collected and processed personal data under a jointly agreed purpose and methodology they were deemed joint data controllers. However, where the parties collected the data together but then used the data for different purposes, they were likely to be deemed 'controllers in common'.

The concept of 'controllers in common' as it was previously understood in the UK is not explicitly referenced under the GDPR or the Data Protection Act 2018, but neither is the concept of 'independent controllers'. The GDPR only explicitly references controllers and joint controllers, although the concept of 'independent controllers' is

widely used by organisations across Europe.

It is important to note that both parties in a joint controller relationship will be subject to controller obligations under the GDPR. In addition, Article 26 expressly requires joint controllers to determine their respective responsibilities for complying with these 'controller' obligations in a transparent manner. Joint controllers should take particular care around allocating responsibility for dealing with data subject rights and providing fair processing information (which should include information about the allocation of responsibility).

As noted above, joint controllers are also jointly and severally liable for compensating data subjects in respect of any non-compliance with the legislation. Joint controllers are also each fully accountable to supervisory authorities for non-compliance.

Consequently, it is understandable why many organisations to date have sought to avoid falling within the definition of joint controllership, and in order to do so, it is important that the limits of that definition are clearly understood.

Case law examples and regulatory guidance

Unfortunately, there is a lack of clear guidance surrounding what does and does not constitute a joint controller relationship. Previous guidance has supported a relatively narrow interpretation of the definition of joint controllers under Article 26, which has been reflected in market practice. This may be illustrated by the following 'official' examples:

> ***"This case further lowers the threshold for joint controllership and suggests that any use of a social media platform by a company, such as setting up a YouTube Channel or Twitter account, may constitute a joint controller relationship to the extent that the platform processes the personal data of the company's subscribers."***

Example 1

The European Commission has given the following example of a joint controller relationship.

A company offers babysitting services via an online platform. The company has a contract with a third party which allows it to offer value-add services, such as parents being able to rent games and DVDs that the babysitter can bring. Both companies are involved in developing the online platform, and both will process client personal data in order to provide these combined services.

The companies jointly decided the purposes and means of the processing, and as such are joint controllers.

Example 2

Guidance from the UK Information Commissioner's Office ('ICO') contains an example of a luxury car company which collaborates with a designer fashion brand to host a co-branded promotional event. Attendees can enter a prize draw by entering their name and address into the prize draw system. After the event, the companies post the prizes to the winners. They do not use the personal data for any other purposes.

Here the companies are joint controllers of personal data processed in connection with the prize draw, because they both decided the purposes and means of the processing.

Example 3

The above examples mirror examples provided under the previous legislation, such as the former Article 29 Working Party's example of a travel agency, a hotel chain and an airline setting up an online platform for holiday bookings. The parties agree on the means of processing data (e.g. how they will be stored), and agree to share the data between themselves for the purposes of combining marketing communications. All three parties have jointly agreed the purposes and means of the processing, so are joint controllers in respect of the online platform's processing operations (but are independent controllers with regard to other processing activities, such as the travel agency's excursion booking activities).

All of these examples would seem to align with the definition in Article 26 of the GDPR, i.e. a joint controller relationship will only exist where the controllers jointly determine the purposes and means of processing. However, other guidance and case law now seems to undermine the restrictive interpretation which the market has adopted to date.

Example 4

Within the same piece of ICO guidance, there is the example of a property management company which operates student halls of residence for a university. The company enters tenancy agreements with the students on the university's behalf, and collects rent, which it passes to the university less a commission.

The ICO characterises this relationship as a joint controller relationship, as the company decides what information it needs from the residents to set up and manage the tenancies, but shares this data with the university. Prior to the publication of the ICO's guidance, a relationship of this sort would likely have been deemed an independent controller-controller relationship, given that whilst the purpose of the processing — to manage the properties and collect rent — may be jointly determined, the university ap-

(Continued on page 8)

(Continued from page 7)

pears to play no part in determining what information the company collects nor how it processes it. In addition, the property management company is a business with profit incentives of its own. It is likely that the company collects certain data for its own business purposes quite separate from the university. However, according to the ICO guidance, it seems that it is the sharing of data by the management company to the university which somehow renders this a joint controller relationship.

Example 5

In 2018, in the Wirtschaftsakademie 'Facebook Fan Page' case (C-210/16), the CJEU held that companies which create fan pages on the Facebook platform are joint controllers with Facebook. Creating fan pages allows Facebook to process the personal data of visitors to the fan page (primarily via placing cookies on visitors' devices). Fan page administrators also define parameters which Facebook uses to provide those administrators with statistics about visitors to their fan page. The CJEU decided that fan page administrators therefore take part in the determination of the purposes and means of the processing of the personal data, rendering them joint controllers.

Whilst this case does seem to reflect the Article 26 definition more closely (compared to the Facebook 'Like' plugin case, for example), it further lowers the threshold for joint controllership and suggests that any use of a social media platform by a company, such as setting up a YouTube Channel or Twitter account, may constitute a joint controller relationship to the extent that the platform processes the personal data of the company's subscribers.

Example 6

Later in 2018, in the Tietosuojavaltuutettu case (Case C-25/17), the CJEU extended the scope of joint controllership even further. This case centered around whether the Jehovah's Witness Community, and Jehovah's Witnesses who engaged in door-to-door visits, were controllers in respect of personal data collected by Jehovah's Witnesses in the course of those door-to-door visits. These data were recorded 'informally' by individual Jehovah's Witnesses (rather than being stored in a central database accessible to the wider organisation, for example), but was shared with others to coordinate visiting activities, or to identify households which did not want to be visited again. The data were recorded without the data subjects' knowledge, and included sensitive data about their religious beliefs.

The CJEU held that the Community and the individual Jehovah's Witnesses were joint controllers in respect of personal data gathered from door-to-door visits, regardless of the way in which such data were processed and how many people had access to the data, and regardless of the fact that individual missionaries determined the purpose and means of processing the data, rather than the Community doing so as a collective.

This case widens the scope of joint controllership even further. The Community and the individual Jehovah's Witnesses do not appear to have jointly determined the purposes nor means of this processing, and the Community had even stated that it did not require missionaries to collect personal data. As such it is difficult to see how these activities fall within the scope of the Article 26 definition.

Conclusion

Given the seemingly increasingly wide definition of joint controllership, and the lack of definitive, consistent case law or guidance, there is now a considerable degree of uncertainty associated with categorising data-related arrangements as independent controller relationships. Whether or not organisations consider that any given arrangement falls within the meaning of joint controllership, they would be well advised to ensure a contemporaneous record is kept as to how the parties have categorised the relevant relationship and why.

However, before organisations re-evaluate or re-paper all of their existing controller-controller relationships, and instead of assuming that all arrangements made going forward will be classed as joint controller relationships, it seems sensible to wait and see how the most recent case law is treated in practice.

In particular, for UK organisations and those subject to UK law, it is important to remember that both the Fashion ID case and previous joint controller cases are European cases: there has not yet been a UK joint controller case in this area. Given this, and the uncertainty which now surrounds joint controllership, we may reasonably expect guidance to be issued in due course to clarify the scope of the definition. Indeed, 'Guidelines on concepts of controller and processor (Update of the WP29 Opinion)' features on the European Data Protection Board's Work Programme for 2019/20. We can only hope that if guidance is forthcoming on the definition and concept of joint controllers, it does not stop there, and instead goes on to provide much sought after guidance to organisations regarding the nature of the 'arrangement' which must be entered into between joint controllers in order to satisfy the requirements of Article 26 GDPR.

Duc Tran and Laura Adde
Herbert Smith Freehills LLP
duc.tran@hsf.com
laura.adde@hsf.com