Proskauer

Growing Risks to Corporate Groups and the Global PE Industry from Robust European Privacy and Cybersecurity Enforcement

Proskauer on Privacy Blog on **March 17, 2022**

Since the EU General Data Protection Regulation ("**GDPR**") came into effect in May 2018 there have been numerous high-profile enforcement actions (~US$880m is the largest GDPR fine to-date) and private litigation (including class-action type claims). Notable fines have included the ~US$25m fine levied in October 2020 by the UK's GDPR regulator against Marriott International for alleged cybersecurity failures in connection with its acquisition of Starwood Hotels. Still, the GDPR exposure for corporate groups and the private equity ("**PE**") industry (whether or not established in Europe) continues to expand – notably, from a growing focus on so-called "parental GDPR liability".

In late 2021, Ireland's GDPR regulator and the European Data Protection Board ("**EDPB**") (the collective of EU privacy regulators) applied the parental liability doctrine to calculate WhatsApp Ireland's fine (of ~US$255m) by reference to the global revenues of its parent company (Facebook, Inc.). In addition, parent companies and PE sponsors may now be subject to direct enforcement action with respect to GDPR infringements committed by (even minority-held) affiliates or portfolio companies (even if the parent was not "personally" implicated in the infringement). In turn, corporate groups, PE sponsors and portfolio companies may need to, where appropriate, consider their liability exposure and implement risk mitigation measures.

I. GDPR fines and parental liability

Parental GDPR liability is typically considered to arise in two circumstances, where:

- GDPR fines are *levied on infringing affiliates or portfolio companies* and calculated as a proportion of the annual worldwide revenues of the "undertaking" (i.e., the parent company or PE sponsor). This circumstance directly arose in the *WhatsApp Ireland* case*;* and

- *Parent companies or PE sponsors are directly fined* for GDPR infringements committed by their affiliates or portfolio companies that comprise part of the relevant "undertaking" – including where the fines are calculated as a proportion of the annual worldwide revenues of that "undertaking".

Specifically, depending on the GDPR infringement in question, companies may be fined up to:

1. the greater of: EUR10m or 2% total worldwide annual revenues of the "undertaking"; or
2. the greater of: EUR20m or 4% total worldwide annual revenues of the "undertaking".

In turn, the key concept for parental GDPR liability is that of an "undertaking"

II. The meaning of "undertaking"

The GDPR refers to EU competition law jurisprudence to understand the concept of an "undertaking". EU case law establishes that where a parent company (or potentially a PE sponsor) holds all, or nearly all, the shares in a subsidiary, a rebuttable presumption arises that both companies are part of an "undertaking". With respect to lower levels of investment, the key is whether the shareholder is in a position to exercise "decisive influence" over the subsidiary entity's commercial policy. While the existence of "decisive influence" is fact-specific, relevant factors include (for example) the parent company or PE sponsor's:

- *Veto rights*: Veto rights relative to the affiliate or portfolio company's budget, business plan, operational investments or the appointment of senior management are relevant factors. The crucial element is whether the right is sufficient to enable the parent company or PE sponsor to influence the strategic business behavior of a venture. Importantly, the mere existence of a veto right, even where not exercised, can be sufficient to establish "decisive influence";
- *Right to appoint board members*: The right to appoint independent non-executive directors with observer roles (rather than executives with management power) is less indicative of "decisive influence"; and
- *Power to have personal data protection rules implemented within a company.*

To illustrate, “decisive influence” has been held to exist (under EU competition law) with a minority shareholding as low as 30% (for example, in the *Fuji* case, where there were common directors). Similarly, in the *Prysmian* case (under EU competition law), the investor was fined EUR37.3 million for the power cable cartel in which the company in which it had invested had engaged due to the “decisive influence” that was held to exist. The investor’s interest in the company through a fund vehicle was only approximately 33%, but its voting rights were far higher (at one point 100%) and it controlled the composition of the board of directors.

III. The *WhatsApp Ireland* case and corporate group structures

The WhatsApp Ireland fine marked perhaps the first time that the parental liability doctrine had been explicitly and publically implicated in a GDPR enforcement context. Notably, the fine was increased four-fold to ~US$255m to reflect Facebook, Inc.’s (larger) revenues rather than WhatsApp Ireland’s (lower) revenues. Significantly, the EDPB was clear that the revenues of “an undertaking was not exclusively relevant for the determination of the maximum fine amount … but it may also be considered for the calculation of the fine itself.”

Importantly, while the fine in this case was imposed on WhatsApp Ireland (not Facebook, Inc.), the EDPB stated (citing EU competition law): “…conduct of the subsidiary may be imputed to the parent company, without having to establish the personal involvement of the latter in the infringement. In particular, the parent company may be held liable for the fine.” Therefore, in future cases, the parent company or PE sponsor may potentially be directly fined for GDPR infringements committed by an affiliate or portfolio company.

IV. Mitigating parental GDPR liability risks

Proskauer’s Private Equity and M&A, Privacy and Cybersecurity, and Antitrust Groups work with corporate groups, PE sponsors and portfolio companies to assess and mitigate parental GDPR liability.

Risk mitigation strategies could include (where appropriate):

- considering whether a group structure or a PE investment would create or has created an “undertaking”;

- determining whether investor rights that might confer “decisive influence” are necessary to accomplish business objectives, and if not, identifying ways to limit potential for a finding of “decisive influence”;
- determining, through appropriate due diligence, the extent of any GDPR compliance gaps across a corporate group or portfolio companies, and remediating such gaps pre or post-transaction; and
- obtaining appropriate GDPR-related warranties and indemnities, and post-closing covenants.

Check back here for further developments on these growing enforcements risks to corporate groups and the global private equity industry.

View Original