Client Update
Draft EU Guidelines on Cross-Border Data Transfer

Earlier this month, the Article 29 Data Protection Working Party (a coalition of European Union member states' data protection regulators) issued draft Guidelines on when EU personal data can be transferred to non-EU countries that, according to the EU authorities, do not adequately protect personal data. The Guidelines interpret Article 49 of the EU General Data Protection Regulation ("GDPR"), which deals with these types of transfers. Although not legally binding, the Guidelines suggest how EU data protection authorities will interpret Article 49. The comment period for the Guidelines is open until 26 March 2018, providing businesses and other stakeholders with an opportunity to influence the final version.

Under the GDPR, EU personal data can be transferred outside the EU only if the recipient country is certified by EU authorities as providing an adequate level of data protection, or if EU-approved safeguards for such protection, such as standard contractual clauses or binding corporate rules, have been implemented. Article 49 provides exemptions (or "derogations") in certain limited circumstances.

The Guidelines bring some good news to companies required to produce EU personal data to civil litigants or enforcement authorities outside the EU, and in the United States in particular. However, the Guidelines maintain the Working Party's restrictive interpretation of other derogations. That means that the GDPR, as currently interpreted, likely will restrict cross-border data sharing even in some cases when important interests like cybersecurity are at stake.

THE GOOD NEWS: "ESTABLISHMENT, EXERCISE OR DEFENCE OF LEGAL CLAIMS" DEROGATION MAY ALLOW FOR GREATER INFORMATION SHARING WITH U.S. AUTHORITIES AND CIVIL LITIGANTS[1]

Under Article 49(1)(e) of the GDPR, EU personal data can be transferred to the U.S. if it is necessary for the establishment, exercise, or defence of legal claims. The Working Party's interpretation of the analogous article in the Data Protection Directive (the GDPR's predecessor) offered only one example where this derogation "appears to" apply: an active U.S. litigation against a company by its employee that requires transfer of that employee's personal data from the EU. Any such transfer also had to comply with relevant international conventions, including the Hague Convention on Taking of Evidence. Unsurprisingly, many practitioners expressed doubt that this provision could be used as a basis for complying with pre-trial civil discovery requests or in non-adversarial dealings with U.S. authorities.

The new draft Guidelines take a more expansive view of this derogation. They state that a transfer of EU personal data to the U.S. could be made when it is necessary for a U.S. criminal or administrative investigation, for the purposes of defence or to obtain "a reduction or waiver of a fine legally foreseen," or for pre-trial discovery. The Guidelines interpret Article 49(1)(e) to require a "formal, legally defined process" in the U.S., but emphasise that this "covers a range of activities."

Assuming that the draft Guidelines do not materially change before they are formally adopted, Article 49(1)(e) could serve as a basis for producing information to the U.S. Department of Justice ("DOJ") or the U.S. Securities and Exchange Commission ("SEC") in connection with the Foreign Corrupt Practices Act or other white collar matters. In fact, the Working Party appears to have had just such matters in mind; the Guidelines specifically refer to antitrust, corruption, and insider trading investigations. That said, the requirement that "formal procedures" have been instituted (or at least be impending) suggests that voluntary self-disclosures to the DOJ or the SEC are unlikely to be covered.

To rely on Article 49(1)(e) to transfer EU personal data, companies must show that the transfer is necessary. The Guidelines state that U.S. authorities' "mere interest" in the data or "possible 'good will'" to be obtained from the production will not meet that standard. If a U.S. subpoena calls for the production of a specific EU individual's personal data—for example, if the individual is suspected of wire fraud or money laundering—transfer of that personal data presumably would qualify. On the other hand, producing personal data of other EU individuals who may have transacted with the alleged fraudster, but who are not themselves targets of the U.S. subpoena, might run afoul of the necessity requirement. Such data may need to be anonymised

[1] The Guidelines and Article 49 of the GDPR apply to all transfers to countries that do not provide an adequate level of data protection. In practice, however, they tend to target transfers to the U.S., given the breadth of U.S. civil discovery and the extraterritorial reach of U.S. law. Accordingly, we refer to transfers to the U.S. throughout this update.

or pseudonymised before it is transferred. Where the EU personal data is not explicitly requested by the U.S. legal process but is likely of interest to the requesting party, companies may consider engaging with the U.S. authorities or civil litigants to modify the relevant requests to meet the requesters' goals while satisfying the GDPR.

By making room for these considerations, the draft Guidelines provide a path for multinational companies to navigate between U.S. information requests and the GDPR, a path that previously was difficult to discern.

THE BAD NEWS: PUBLIC INTEREST, VITAL INTERESTS, AND COMPELLING LEGITIMATE INTERESTS BASES FOR DATA TRANSFERS REMAIN HIGHLY RESTRICTIVE

The Guidelines fail to offer a broader interpretation of other bases for EU personal data transfer to the U.S.. As before, the Guidelines limit the "public interest" derogation to instances when the transfer itself is in the public interest of the EU, for example, because of an agreement between the EU and the U.S. to share particular types of information. A general shared interest (for example, that both the EU and the U.S. seek to combat terrorism or money laundering) is insufficient.

Likewise, the "vital interests of the data subject or others" basis for data transfers continues to be limited to medical emergencies and other life-and-death situations when the relevant individual is incapable of giving consent. The Guidelines do not consider other serious risks to individuals that may be prevented or ameliorated through cross-border data sharing. Cyberattacks are a prime example. As financial institutions and other businesses fighting against cyber-threats can attest, a timely and free exchange of attack-related data, which may include personal data of suspected perpetrators or their victims, is crucial to preventing or stopping the attack.

The Guidelines appear to consider cyber-related data transfers under Article 49's "last resort" derogation—that for "compelling legitimate interests" of the data transferor. They state that a business may be "compelled to transfer the personal data in order to protect its organisation or systems from serious immediate harm." The Guidelines emphasise, however, that the "compelling legitimate interests" must be those of the data transferor, not of the data importer or any other third party. This would prevent an EU financial institution hit by a cyberattack from transferring relevant EU personal data to a U.S. financial institution to prevent the attack from spreading to the latter. That transfer would be in the interest of the data importer, not the data transferor. While one can hope that this is not the type of a situation where the EU data

protection authorities would take action against the data transferor, the fact remains that Article 49 provides little cover for such transfers.[2]

It is possible that the Working Party will reconsider its interpretation of Article 49, either during the comment period or subsequently. In an unusual move, the Working Party explicitly stated that it would review and update the Guidelines, if needed, based on practical experience of their application. In the meantime, companies would be well advised to consider other bases for cross-border information sharing, such as by executing standard contractual clauses among relevant industry participants.

Debevoise advises businesses, both in and outside of the EU, on all aspects of GDPR preparedness.

* * *

[2] Article 49 places additional restrictions on the "compelling legitimate interests" derogation, including that any such interests must be weighed against the rights of the affected individuals and that any transfers under this derogation must be notified to the relevant data protection authority and affected data subjects.

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

James J. Pastore
jjpastore@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Chris Garrett
cgarrett@debevoise.com

Ayushi Sharma
asharma@debevoise.com

FRANKFURT

Thomas Schürrle
tschuerrle@debevoise.com

Friedrich Popp
fpopp@debevoise.com