Confederazione Italiana della Piccola e Media Industria Privata
00186 Roma - Via della Colonna Antonina, 52
tel +39-06-69015.1 fax +39-06-6791488
www.confapi.org - info@confapi.org

Privileged and confidential

THE EUROPEAN DATA PROTECTION BOARD'S RECOMMENDATIONS ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS

Introduction – Why EU Companies Should Care and Respond

On 10 November, the European Data Protection Board (EDPB) issued, for public consultation until 21st December, its *Recommendations* on measures to promote compliance with the EU Court of Justice's recent decision in *Schrems II*. The Court in *Schrems II* held that organisations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries.

The proposed *Recommendations* propose a prescriptive, non-risk-based approach that goes far beyond the requirements of *Schrems II*.

If the *Recommendations* are adopted in their current form, any organisation that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question. They also will require EU organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for most small and medium-sized enterprises, research institutions, and others.

As a result, the *Recommendations* will make it highly risky for EU companies to engage in commerce with non-EU customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine and necessary operational tasks. The potential negative effects on EU competitiveness, innovation, and society are enormous.

By focusing only on non-adequate jurisdictions, the *Recommendations* threaten to create an unequal international playing field for data protection, where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them. Such discriminatory treatment of different jurisdictions is also likely to invite retaliation by jurisdictions whose companies are placed at a competitive disadvantage in European markets by the EDPB's actions.

The EDPB has given interested parties until only 21st December to provide their views. This means that all stakeholders must act quickly to express their concerns.

The goals

Among the points that European companies and trade associations might wish to raise with the EDPB are the following:

1. ***The Recommendations should allow data exporters to take account of the full context of a transfer.***

In *Schrems II*, the Court indicated that data exporters should consider the full context of a transfer when evaluating its legality—specifically, that transfers should be evaluated "in the light of all the circumstances of that transfer" (¶¶ 121, 146) and "on a case-by-case basis" (¶

Confederazione Italiana della Piccola e Media Industria Privata
00186 Roma - Via della Colonna Antonina, 52
tel +39-06-69015.1 fax +39-06-6791488
www.confapi.org - info@confapi.org

134). Several passages in the *Recommendations*, however, appear to foreclose this contextual approach.

2. ***The Recommendations should propose technical measures that are workable in practice.***

The *Recommendations* propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the *Recommendations'* case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

3. ***The Recommendations should clarify that contractual measures may provide sufficient safeguards.***

Although the *Recommendations* propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organisational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires (¶ 48). This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.

4. ***The Recommendations should make clear that enforcement by supervisory authorities will be measured and appropriate.***

The Court's holding in *Schrems II* was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation.