McKinsey & Company

Risk & Resilience Practice

International personal-data transfer amid regulatory upheaval

The Schrems II ruling created a noteworthy disruption in the data-privacy environment. Here, we outline a risk-based approach to managing uncertainty from the ruling.

by Oliver Bevan, Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson

March 2021

In mid-2020, the data-protection landscape experienced a major disruption. The Court of Justice of the European Union (CJEU) issued a ruling with wide-ranging implications. The ruling, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (or "Schrems II"), has now cast doubt on all personal-data transfers between the European Union and other markets with lower levels of data protection, most notably the United States. The ruling creates significant uncertainty for organizations that have personal data on customers, employees, or other so-called data subjects in Europe and also have any connections or data transfers outside the European Union—that is, virtually all global organizations.

In response, the European Data Protection Board (EDPB), the cooperation forum for European data-protection regulators, recently issued a draft guidance for companies, and the European Commission published a draft update of the standard contractual clauses to be used in personal-data-transfer situations to recipients outside the European Union. Organizations have a year after the final adoption of the European Commission's decision to come into compliance, or they risk fines of up to 4 percent of worldwide revenue, in line with provisions of the General Data Protection Regulation (GDPR).

The issue has strategic implications affecting business operations, IT infrastructure, marketing, HR, research and development, and other functions. In this article, we discuss potential short- and long-term measures that companies can take, and we define a means of dealing with similar situations in the future. Schrems II is a significant disruption, and it points to a more complex data-privacy environment with increasingly demanding local requirements. The steps that companies take today will have significant implications—both positive and negative—in the future.

Invalidation of the Privacy Shield

The European Union and the United States have different regulatory standards for how organizations must protect the personal data they hold. Before the Schrems II ruling, US companies could transfer data about consumers and employees in the

Companies need to identify the ongoing transfers and the markets among which the transfers occur as a starting point to identify possible scenarios and define proper lines of action.

European Union under an agreement between EU and US authorities known as the Privacy Shield. US companies could self-certify and use the Privacy Shield as a valid legal basis for receiving data from the European Union without putting in place any additional protections. In July 2020, however, this arrangement was declared invalid by the CJEU.

Given the significant amount of data that flow between the European Union and the United States, the ruling has upended many companies' data-protection policies and practices concerning data transfers and has led to significant uncertainty. Companies transferring personal data outside the European Union are now struggling to define a roadmap for interpreting the ruling and ensuring that future transfers are compliant.

That uncertainty is reflected in a recent client survey that McKinsey conducted. Among participants, 47 percent said that they are not sure they could guarantee a sufficient level of data protection in a post–Schrems II environment, and another 11 percent said they did not have clarity. In addition, 40 percent had launched a project to implement additional safeguards, but nearly as many (35 percent) were waiting for further guidance from regulators (Exhibit 1).

Regulatory guidance, but no clear answers yet

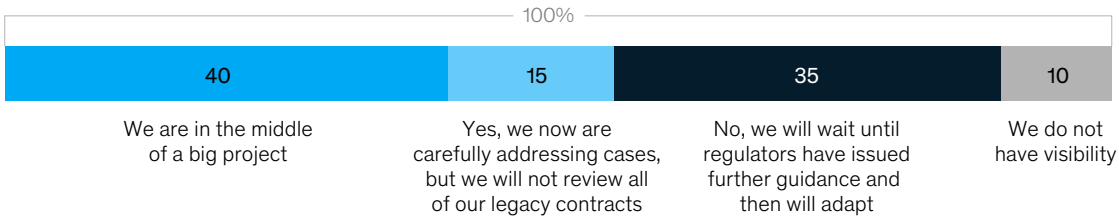
As mentioned earlier, to clarify the situation, the European Commission has issued updated standard contractual clauses aimed at meeting at least

Exhibit 1

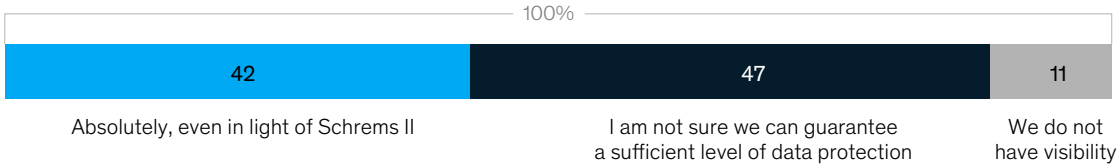
Post the Schrems II ruling, a majority of surveyed participants expressed uncertainty about guaranteeing sufficient data-protection levels.

Respondents' reactions after the Schrems II decision, %

QUESTION: Are you doing something about Schrems II with regard to standard contractual clauses (eg, implementing additional safeguards)?



QUESTION: Are you confident your IT security is (still) sufficient after the Schrems II decision?



Source: McKinsey Roundtable Survey, October 7, 2020

some of the required supplementary measures requested by the CJEU. In addition, to help companies navigate the uncertain landscape, the EDPB issued a six-step roadmap for them to follow (Exhibit 2). Despite good intentions, these measures do not remove the uncertainty around EU–US transfers.

For example, the six-step approach outlined by the EDPB is theoretically sound, and many companies will recognize the steps from previous GDPR implementation work: companies initially map all transfer processes and identify the relevant transfer mechanism. However, the updated version from the EDPB includes two new steps for most companies (numbers three and four). Both of these are quite broad and therefore warrant a closer look.

Step three: Assess effectiveness of transfer tool

Step three in the EDPB's six-part roadmap recommends that a company assess the laws in the recipient country to determine whether its current transfer processes are sufficient or if there is a risk of disclosure of personal data to public authorities. Though both the European Commission and the EDPB provide examples on how organizations should do so, neither provides the level of clarity many organizations require to develop appropriate approaches—for example, by providing an assessment of countries or outlining the risks for different sectors in different markets. In fact, there are some contradictions in the two initial approaches, with the European Commission recommending a risk-based approach whereas the EDPB specifically asks companies to focus on the legal landscape rather than conducting a risk assessment. Even setting this discrepancy aside, legal professionals may struggle to make sense of the legal landscape in a foreign country.

Step four: Adopt supplementary measures

In step four of the revised EDPB approach, after performing the country assessment, companies should consider and adopt supplementary measures—contractual, technical, organizational—to minimize or remove the risk of foreign authorities accessing personal data. Again, although both the EDPB and the European Commission give a long list of potential measures that organizations

Exhibit 2

The European Data Protection Board issued a six-step roadmap to help companies navigate the data-privacy disruptions caused by Schrems II.

European Data Protection Board's six-step roadmap for data transfers

Source: Recommendations by the European Data Protection Board, adopted on Nov 10, 2020

could use, they don't provide clear steps that companies likely need to take.

Tailoring the right response

Given the lack of clarity, we believe companies need to identify the ongoing transfers and the markets among which the transfers occur as a starting point to identify possible scenarios and define proper lines of action. Longer term, companies should consider reviewing the necessity of data transfers between the European Union and the United States, or other markets with challenging legal environments, and potentially reassess these transfers.

More immediately, however, companies should consider moving forward with a set of short-term organizational, contractual, and technical measures outlined below.

Organizational measures

Among organizational measures—including governance and reporting—we recommend that the data-protection office follow developments as the situation continues to evolve and communicate that information to the C-suite. It is important that the company's senior leadership is made aware of the situation, including the potential for disruptions to the business and the penalties for noncompliance.

This new environment presents fundamental operational challenges that require a coordinated, strategic response. Organizations could address that by assembling a cross-functional team that can assess the situation and develop the response. This team can be the company's current data-protection organization, with input from other functions, but the current situation could also present an opportunity to build a broader team that can define and implement appropriate organizational, contractual, and technical measures required not only within the company but also from recipient organizations. Key capabilities required in the team include legal, data protection, HR, marketing, and—critically—representatives from the business.

Contractual measures

The guidance from the EDPB and the European Commission decision outlines several new contractual obligations, which entail new work processes and reporting lines within a company. Before entering into contractual arrangements, it would be worthwhile to think these through to ensure the selected approach is functional and meets new requirements—for example, who is the point of contact between the cooperating companies, what are the reporting lines, and which actions should be taken in specific situations (such as if the recipient company gets a request for disclosure or if there are changes to the legal landscape)? Only after that point should companies consider replacing current standard contractual clauses and binding corporate rules for all data transfers between the European Union and the United States.

Technical measures

Most technical solutions require a long implementation time, but companies could use the current window to develop a roadmap of future steps. These include protection measures such as encryption and pseudonymization with keys stored on European soil and potentially leveraging local cloud providers and local data centers. In addition, companies can consider tools (or organize operations) that do not require storage within countries with challenging legal landscapes and, instead, localize operations within countries that have adequate data-security requirements (as deemed by the European Union). All of these measures may lead to larger-scale changes of the company's IT architecture.

Future changes to the global data landscape

The CJEU decision in the Schrems II case is situated within a broader global landscape of a splintering internet due to a host of technological, geopolitical, and regulatory factors including data-localization laws or draft laws in countries such as China, India, Russia, and Saudi Arabia. In addition, Brexit might raise similar questions about data transfers to and from the United Kingdom, depending on the

outcome of the European Commission's adequacy assessment. Regardless of how companies address the Schrems II ruling, they need a clear approach to meet similar regulatory challenges in the future.

Our experience shows that an analysis based on an evaluation grid can help detail possible scenarios and implications. Specifically, a grid can help structure the analysis of relevant processes against various options for tackling data-privacy and localization requirements, including regulatory or technical solutions, stopping data transfers or operations in a certain country, or other measures. Once a company defines a set of potential solutions, it can assess them by considering legal, reputational, operational, and financial risks. By structuring the various options, companies can determine how to best react to different regulatory changes and plot the best path forward.

The Schrems II decision has major implications for virtually all global organizations that have operations, customers, employees, or other data subjects in the European Union. The future will be shaped largely by developments and decisions by the CJEU and additional guidance from the European Commission, regulators, and national courts, but companies should not wait. Instead, they should address the challenge head-on by taking several short-term measures and considering longer-term options as well. Schrems II is a major case, but it will not be the last data-privacy disruption. By proactively taking strategic, technical, legal, and organizational steps, companies can build up critical capabilities, reinforce customer and employee trust, and prepare themselves for a more volatile data-privacy environment in the future.

Oliver Bevan is a partner in McKinsey's Chicago office, **Daniel Mikkelsen** is a senior partner in the London office, **Henning Soller** is a partner in the Frankfurt office, and **Malin Strandell-Jansson** is a senior expert in the Stockholm office.

Designed by McKinsey Global Publishing