Workday Comments on the European Data Protection Board's Recommendations 01/2020

December 10, 2020

Workday appreciates the opportunity to provide feedback on the European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data on cross-border data transfers (the "Recommendations"). Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 60 percent of the Fortune 50. Headquartered in Pleasanton, California, Workday has more than 12,300 employees worldwide and 21 offices across Europe.

At Workday, we believe that privacy is a fundamental right. We are deeply committed to protecting our customers' privacy and strive to be a productive partner with EU data protection and policymaking bodies. At Workday, privacy protections have been a fundamental component of our services from the very beginning. Our third-party audit reports and standards certifications provide tangible evidence of how we protect our customers' data. All new offerings include privacy by design from the very beginning of our development processes. Workday was the first organization to adhere to the EU Cloud Code of Conduct and the first company to certify to the APEC Privacy Recognition for Processors (PRP) system. And we've built features that enable our customers to comply with GDPR.

Guidance from regulators helps both organizations and individuals understand how those who enforce the General Data Protection Regulation (GDPR) understand its provisions and what steps may be needed in order to comply with those requirements. In Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (the "*Schrems II*" case), the CJEU upheld the use of Standard Contractual Clauses to transfer personal data to third countries, while indicating that supplemental measures may need to be taken where the law in the third country is not "essentially equivalent" to EU law in the protections it provides related to government access to data. This is precisely the type of area where further guidance from the EDPB is welcome.

Moreover, in our view, the EDPB adopts a sensible framework for how data exporters and data importers should evaluate those transfers. Specifically, the Recommendations set out a six-step process: (1) know your transfers, (2) identify the transfer tool relied upon, (3) assess whether that tool is effective in light of the circumstances of the transfer, (4) adopt supplementary measures, (5) procedural steps related to effective supplementary measures, and (6) re-evaluate at appropriate intervals. This framework ensures that transfers are known, an appropriate transfer mechanism is employed, additional protections are implemented as needed, and changes made as laws and transfers evolve.

Unfortunately, the EDPB goes on to apply this process in a manner that is overly-restrictive in light of the CJEU judgment in *Schrems II*. When read in their entirety, the Recommendations adopt the following logic: if a third country law permits any government access that would not be permitted under EU law, the data importer must ensure, via technical means, that no such access can ever occur. The Recommendations

take this approach regardless of whatever contractual commitments the data importer may make, regardless of whatever organizational measures it has put in place, regardless of the history (or lack thereof) of access to the data being transferred, and regardless of any consideration of the risk of improper access as measured against European law. The result is a theoretical approach to data transfers that simply does not work in the real world and, more pertinently, does not enhance protection of individuals' data.

The *Schrems II* Ruling

In the *Schrems II* case, the CJEU held that the SCCs could be used for transfers to third countries that didn't offer an adequate level of data protection, but that where governments could access transferred data, the parties must assess on a case-by-case basis whether the data importer could comply with the SCCs. It is worth quoting what the CJEU said specifically on this point, in Paragraph 134 of its decision:

> In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, *on a case-by-case basis* and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, *of personal data transferred* pursuant to standard data protection clauses, by providing, *where necessary,* additional safeguards to those offered by those clauses. (emphasis added)

Three things stand out in this paragraph. First, the assessment of transfers required by *Schrems II* is "case-by-case;" that is, it must take account of all of the specifics of the transfer. While one element of that assessment is the country to which the data is transferred, the law of the country alone is not determinative under *Schrems II*; otherwise, the CJEU would not have upheld transfers to the U.S. pursuant to the SCCs at the same time it was striking down Privacy Shield. Second, the analysis of whether the country's law provides adequate protection must relate to the "personal data transferred." The nature and type of data are core to any analysis of a transfer under *Schrems II*, not ancillary to it. Third, the parties must put in place additional safeguards but only "where necessary."

Once the parties have conducted this case-by-case analysis, considering the personal data transferred, and put in place any supplementary measures, the question becomes how can they determine whether those measures are sufficient to meet the requirements of *Schrems II*. The CJEU answers this question in Paragraph 137 of its decision:

> . . . [S]uch a standard clauses decision incorporates effective mechanisms that make it possible, *in practice,* to ensure compliance with the *level of protection required by EU law* and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. (emphasis added)

Here the CJEU sets out a pragmatic test for compliance. The companies must ensure that "in practice" the data importer can provide "the level of protection required by EU law." In this paragraph, the CJEU recognizes an obvious truth: no supplemental measure is foolproof. For this reason, absolute certainty regarding government access isn't the standard. Put another way, the CJEU, in the *Schrems II* decision, doesn't consider theoretical possibilities, but instead is focused on an assessment of what happens in the real world. This follows from the CJEU's framing of the issue in Paragraph 126, where it stated that "there

are [situations] in which the content of those standard clauses might not constitute a sufficient means of ensuring, *in practice*, the effective protection of personal data transferred to the third country concerned." (emphasis added). No access ever occurring simply is not the standard set forth by the CJEU in the *Schrems II* decision.

The EDPB Recommendations

Unfortunately, the EDPB recommendations are not consistent with the case-by-case analysis mandated by *Schrems II*, or its pragmatic test of ensuring compliance "in practice." Instead, the EDPB, under the hallmark of setting out an objective standard, states in Paragraph 42 of the Recommendations that the only thing that matters to the analysis is "legislation publicly available." Indeed, the paragraph goes on to note that parties may "not rely on subjective [factors] such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."

But this is begging the question. Any analysis of a country's law considers not only the text of the law but how it is interpreted and applied in practice. Indeed, the Recommendations themselves, in the very next paragraph (Paragraph 43), take this approach, saying that parties should consider "[e]lements demonstrating that a third country authority will seek to access the data" from the data importer or while it is in transit "in light of reported precedents." If the parties can—indeed must—consider reported precedents when assessing whether data will be accessed, they must equally be able to rely on reported precedents demonstrating a lack of government interest in and access to data of the nature and type transferred. Both the letter of the law and actual practice are objective, not subjective, criteria.

Many countries around the globe, including EU Member States and the United States, have sought access to online data for national security purposes since the dawn of the Internet. We now have a substantial body of practice that makes clear that primarily they are interested in communications and social media data. This makes sense: it is through communications that activities impacting national security are planned, and social media through which actors in those activities are recruited. But lots of personal data transferred from the EU to third countries, including the United States, is not communications or social media data. Much of the data transferred relates to sales and marketing or to human resources. These types of data simply are not of interest to intelligence authorities, regardless of the identity of the data subject, as demonstrated by the utter lack of government access requests, and indeed in the case of the U.S. by affirmative statements of the government itself. Moreover, where data is held by an enterprise cloud provider, in almost all cases the data is first sought from the customer directly; in the case of the U.S., doing so is official government policy.

In sum, where there is no reasonable likelihood of government access, there is no meaningful risk to the privacy rights of the individual whose data is transferred. Above all, GDPR takes a risk-based approach to processing of personal data. Recital 74 states that the controller must implement effective measures and that those measures "should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons." Recital 76 goes on to say that "[t]he likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing." And Article 82 of GDPR embodies this risk-based approach by providing for damages to data subjects, reflecting the reality that on rare occasions unexpected risks will materialize. Consistent with this risk-based approach, where the nature of the data makes it very unlikely to be accessed (regardless of who the data subject may be), transfers pursuant to the SCCs must be permitted.

This is particularly true where the data importer adduces additional safeguards for such transfers. There are a number of such measures companies can and have put into place. Even before the issuance of the European Commission's draft Revised SCCs (see below), Workday committed to challenge all government requests for data where any grounds existed for doing so, as well as to challenge any restrictions on informing affected customers. Other companies offer similar commitments, and some even provide for damages in the event data ultimately must be disclosed in a manner inconsistent with European law.

Again, however, the Recommendations give short shrift to such measures. In Paragraph 48, they state "Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country." It is true that contractual and organizational measures do not bind the third country's government. But it is equally true that such measures can and do make access more challenging, reducing or eliminating disclosures. Here the EDPB again appears to have taken an all-or-nothing approach: unless it is guaranteed any and all access can be blocked, the supplementary measures are insufficient.

For this reason, the EPDB has embraced technical measures, most notably encryption. Encryption can and does provide strong protection against unauthorized access. But like any technology, it is not infallible. The idea that technical measures will guarantee 100% that no improper access by governments will take place simply is not supportable. Indeed, earlier this month the European Council adopted a resolution citing the need to ensure access to data notwithstanding encryption. And yet, even where the risk of access in light of contractual and organizational measures is as low—or even lower because the data are not of interest—as if technical measures were put in place, the Recommendations would not permit transfers if the law of the third country permits access in certain circumstances. Nothing in the *Schrems II* decision mandates this approach; again, as noted above, the measures need simply to ensure that "in practice" the level of protection is equal to that required by EU law. And that level, while high, is not absolute.

The challenges and consequences of this technical measures-only approach can be seen in Use Cases 6 and 7, where the Recommendations state that no effective measures could be found. Use Case 6 is written broadly, and essentially encompasses any cloud computing service, of whatever type, that is more than mere data storage. To provide any value-add beyond storage, the cloud provider must have access to the data unencrypted in order to process it. This is true whether sorting files, sending and receiving emails, processing HR transactions, or managing sales and marketing, to take just a few examples.

Yet many cloud providers offer high security and a high degree of privacy protections; often far more than will be found in data kept locally on a server in the company's offices. They have sophisticated security measures against hacking, well-designed privacy programs that regulate when and how data is processed, controls in place to ensure compliance, all backed by certifications and audits. As noted above, many services do not process data that is of the type that interests national security authorities, regardless of the identity of the individual data subject.

Barring such transfers, where no practical risk of access exists, would deeply impact customers of these cloud services—both those headquartered in Europe and those headquartered elsewhere with European operations—and significantly impede Europe's digital transformation without adding even a modicum of actual, real privacy protection. The scope of the impact is demonstrated by a recent impact survey on *Schrems II* conducted by Digital Europe, BusinessEurope, the European Roundtable, and the European Automobile Manufacturers Association. In that survey, 75% of the companies relying on SCCs for international transfers were European, with 90% of the companies using SCCs using them for business-to-business transfers (not consumer data which as noted above is the focus of interest for government

authorities). Three-quarters of those surveyed using the SCCs use them to transfer data to more than one country, emphasizing the point that this issue goes far beyond just transfers to the U.S.

And suggesting that the data be kept in Europe and not transferred does not solve the problem. First, many multinational companies need their data to be gathered in a single data center region, in order to bring together all of their information for processing transactions. Two systems—one European, one not—that cannot talk to one another (because even if the non-European data were transferred to Europe repatriation abroad would be barred by the Recommendations) breaks business operations. And that presumes that the people who need to see the data are in Europe. As Use Case 7 makes clear, remote access is a transfer, so even access by individuals outside of Europe of data in a European data center falls afoul of the Recommendations as the data cannot remain encrypted once transferred.

Second, even keeping data in Europe does not address the risk of government access if that risk exists simply as a result of a law on the books. U.S. government access laws reach any company that does business in the U.S., even if their data is stored elsewhere: where the company is headquartered is not determinative. And once the E-Evidence Directive is adopted, the access regimes of EU Member States likewise will reach beyond their national borders. At the end of the day, both European companies and European cloud service providers would have to exit their U.S. operations to comply with the approach set out in the Recommendations.

The Revised SCCs

Thankfully, there is a different approach: one that complies fully with the *Schrems II* decision, effectively protects privacy, and allows cross-border data transfers to continue subject to appropriate protections. This approach is reflected in the European Commission's draft Decision on standard contractual clauses for the transfer of personal data to third countries (the "Revised SCCs"). Clause 2 of the Revised SCCs obligates the data exporter and the data importer to determine, on a case-by-case basis, whether the Revised SCCs can be complied with by the data importer. In making this case-by-case assessment, they require the data exporter and the data importer to consider a variety of factors, including among other elements "the nature of the personal data transferred; [and] any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred." In this, the Revised SCCs take an appropriately holistic approach to what constitutes the law of the third country, which requires consideration not only of the applicable statutes, but how they are applied and enforced. Indeed, in Article 45(2) on assessing the level of protection in a third country, GDPR requires the Commission to take into account not only the written law of the third country but consider "as well ... the implementation of such legislation."

And the Revised SCCs enable the data exporter and data importer to put in place additional obligations—whether organizational, contractual, or technical—to guard against such access. These could include things like encryption in transit, to protect against government interception during the transfer; a commitment to challenge any government request to access data and any related restrictions on disclosing such requests; and even damages in the event data had to be disclosed.

In sum, the Revised SCCs fully implement the obligations of *Schrems II*. They require the parties to assess a third country's law in light of its practice; to determine if that law provides adequate protection under the standards of EU law; if it does not, to put in place organizational, contractual, and technical measures to provide a sufficient level of protection; and ultimately to suspend transfers if it is not possible to offer a sufficient level of protection to transferred data. The requirements are strong, reflecting the clear mandate

from the CJEU in *Schrems II*. But they are applied with an eye to the practical effect, which at the end of the day is what matters in safeguarding transferred data and ensuring data protection.

* * *

For all of these reasons, Workday asks the EDPB to reconsider the approach taken by the Recommendations to additional safeguards and to adopt the approach taken by the Commission in the Revised SCCs. That approach ensures a high level of data protection in light of the specifics of the transfer, faithfully implementing the case-by-case approach to data transfers mandated by the CJEU in *Schrems II*. At the same time, it ensures the protections are tailored to the actual, real risk of access in contravention of European law, avoiding the downsides of an overly-restrictive approach and its impact on the ability of companies and individuals to make use of an increasing array of value-added cloud services.

Workday appreciates this opportunity to comment on the European Data Protection Board Recommendations. Please do not hesitate to contact Jason Albert, Managing Director of Public Policy, at ejason.albert@workday.com with any questions or if we can provide further information.