SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
NEO BUILDING
RUE MONTOYER 51
MONTOYERSTRAAT
B-1000 BRUSSELS
BELGIUM
+32.2.504.6400
+32.2.504.6401 FAX

ckerry@sidley.com
(617) 223 0305

BEIJING
BOSTON
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
HOUSTON
LONDON
LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

October 14, 2015

By Hand Delivery and Email

Mr. Frans Timmermans
First Vice-President,
Commissioner for Law and
the Charter of Fundamental Rights

Ms. Vera Jourová
Commissioner for Justice, Consumers and
Gender Equality

Sig. Giovanni Buttarelli
European Data Protection Supervisor

Mme. Isabelle Falque-Pierrotin,
Chair, Article 29 Working Party

Dear Ladies and Gentlemen:

The decision by the Court of Justice of the European Union (CJEU) in the *Schrems* case has precipitated a crisis of uncertainty and complexity concerning transatlantic data transfers. We, therefore, write on behalf of leading American businesses, and as individuals who have been deeply involved in EU-US cooperation and trade, to request that the European Commission and the data protection authorities ("DPAs") that make up the Article 29 Working Party ("Working Party") act without delay to address this difficulty. Specifically, we request that you promptly take the following actions:

1. Reaffirm that the *Schrems* decision does not apply to data transfers pursuant to Model Clauses, Binding Corporate Rules, and derogations in Directive 95/46/EC, and that data transfers may continue pursuant to these mechanisms.

2. Reaffirm that DPAs, before they can conclude that a company infringes data protection rules because of allegedly deficient derogations under Article 26, must assess first whether US laws in force today provide an "essentially

equivalent" level of protection to the current EU legal order, taking into account the specific data transfer operations at issue.

3. Complete negotiations with the United States for a new, strengthened Safe Harbor Framework. After two years of negotiations, the work has been done to complete this agreement, and the detailed information supplied concerning present-day surveillance law in the United States and the measures taken by the United States to protect foreign citizens meet the requirements of necessity and proportionality under EU law and stand up to comparison with the protections in most EU Member States.

4. Initiate a process to conduct the comparison of the legal order in force in the EU with regard to government surveillance with that in force in the United States. This will expedite the "due diligence" that the CJEU indicated is needed for adequacy determinations in this regard and ensure thorough and consistent examinations by DPAs. Such a proceeding should also address prospective adjustments to other data transfer mechanisms (such as adequacy determinations for third countries other than the United States) that are subject to derogations for national security similar to those in the Safe Harbor Framework, Directive 95/46/EC, and other EU legal instruments.

5. Confirm that the more than 4,000 companies that have operated under the Safe Harbor Framework need a reasonable period of adjustment to select and implement alternative transfer mechanisms, protect the interests of all stakeholders involved, and respond in a proportionate way to the Court decision.

These steps are urgent because, as Commissioner Jourová has stated, transatlantic data flows are the "backbone" of the European economy and the Commission has therefore recognized that continuity of these data flows is a priority. Commissioner Jourová's description is well-grounded: the US-EU trade relationship is the world's largest, accounting for approximately one-third of global trade flows supported by flows of digital information for transactions, logistics, supply chain management, customer relations, workforce management, marketing, and many other daily necessities of commerce. (Meltzer, Brookings, 2014). Without Safe Harbor, Model Clauses, and Binding Corporate Rules, the cost to EU GDP is estimated at -0.8% to -1.3%, the drop in EU services exports -6.7%, and the drop in manufacturing exports up to -11%. (ECIPE, 2013). Thus, a disruption of transatlantic data flows will

injure not just many companies that have relied on Safe Harbor, but also their European business partners and customers.

Unless and until a new and firm basis for transatlantic data transfers is established through either a new strengthened Safe Harbor Framework or alternative mechanisms, the basis for such transfers is subject to challenges. In this light, both companies and DPAs face a turbulent period. Allowing an adjustment period that maintains the status quo will provide some stability and certainty. By contrast, shutting off data flows would be disproportionate.

In the Commission press conference following the *Schrems* decision, First Vice-President Timmermans and Commissioner Jourová rightly noted that transatlantic data transfers can continue under Model Clauses, Binding Corporate Rules, or other derogations in Directive 95/46/EC. As discussed in greater detail below, however, moving forward under these alternatives is far from automatic. Indeed, the number and types of questions that have come up in webinars by the International Association of Privacy Professionals and Data Guidance and in other forums joined by thousands of privacy officers and lawyers demonstrate the complexity and multiplicity of decisions companies must make. The challenge and expense of addressing these questions is even more daunting for small-and-medium enterprises (SMEs) without ready access to privacy professionals. Many of these questions will flow through to DPAs.

Without a Safe Harbor Framework, the affected companies will need to make separate evaluations for each kind of data operation or set of data operations. Unless they have the time and resources needed to undertake transfer-specific adequacy determinations comparing current laws in the US and in Europe (Directive Article 25, CJEU ¶70-75), they may have to put in place changes in business and legal practices that may include new contract provisions to reflect Model Clauses, revised business practices and network configurations, new consent forms, updating privacy policies to align with such changes, and applying to DPAs for approval of Binding Corporate Rules ("BCRs"). Companies will need to make these changes with adequate notice and due regard for their customers, suppliers, and subcontractors.

These are not determinations that can be made and implemented overnight.

Consider the following examples:

- BCRs are seen as unsuitable for smaller companies because of the lengthy process of approval and the attendant expense. Multinational companies that have obtained BCRs have reported spending more than $1 million and taking 18 months to complete the process, with the outcome applying only to intra-group data transfers.

- In many Member States including Austria, Belgium, and Spain, Model Clauses must be submitted for approval by DPAs, a process that can take weeks or even months. Model Clauses are neither comprehensive nor flexible; there are still no forms covering transfers from a data processor, nor are they practicable where data is received from hundreds of customers across the EU.

- A particular benefit of cloud services has been to enable SMEs to scale up efficiently with a higher level of functionality, security, and other features than they can achieve themselves. As the Commission has acknowledged in its Digital Single Market Strategy, there are few competitive alternatives for cloud services in Europe. Even if there were, companies that rely on US cloud providers would have to enter into new business and technical arrangements if they are to store and process data in Europe. The same will be true for companies that make other arrangements to store and process in Europe unless they are large and diversified enough that they already have facilities there.

- The smaller the enterprise, the more difficult it is to put in place new mechanisms, not only because of the transaction costs but because they may require complete revision of a company's business model. Take providers of mobile applications, many of them from Europe that market their apps globally through the app stores of manufacturers or providers. A large proportion of these are small start-ups with very small staffs. Thus, they are unlikely to carry lawyers or privacy officers on their payrolls and could face an overwhelming challenge to adapt Model Clauses to a large number of customers or select among derogations on a transfer-specific basis.

In turn, DPAs will face numerous requests for guidance, proceedings for review of BCRs or Model Clauses, complaints from citizens who wish to follow Mr. Schrems' path in challenging various data transfers or transfer mechanisms, and proceedings with respect to data transfers brought pursuant to Article 25 (1) and (2) and Article 26 (2). With hundreds of companies likely to file thousands of Model Clauses, the

approval process may be severely delayed, and DPAs may need to obtain additional resources.

It is evident that their actions will be under close scrutiny. The CJEU made clear that adequacy determinations require a comparison that is transfer-specific of "laws in force" in the US with the "EU legal order." The CJEU's judgment also makes clear that such comparisons must now include the legal orders relating to surveillance by governments. The comparison must assess whether the present-day laws in the United States (as opposed to past newspaper reports) provide an "essentially equivalent" level of protection as compared to that under Directive 95/46/EC, the Treaty of Lisbon, and other laws in Europe. Incomplete European studies of government surveillance have suggested that multiple Member States conduct broad surveillance without notifications or redress. As the CJEU noted, these assessments must be done with "due diligence." The assessments and follow-up also must be consistent with companies' rights under the Charter (e.g. ¶¶ 17, 20, 47) and with international trade laws. There needs to be orderly process, not summary decisions like the rushed decision by the DPA of Schleswig-Holstein. In assessing procedures for adequacy determinations in 1997, the Commission observed that if these authorities are called on to approve specific data transfers in advance or *ex post*, "the shear [*sic*] volume of transfers involved may mean that a system to prioritise the efforts of the supervisory authority will be needed."[1] The prospect of approvals for specific data transfers now comes to the fore. DPAs therefore face a wave of new responsibilities. All these processes will take time.

Adding to the complexity and uncertainty ahead is the prospect of a new Safe Harbor framework. In praising the *Schrems* decision, Chairman Moraes of the LIBE Committee of the European Parliament called for "an immediate alternative" to the 2000 Safe Harbor Framework. Prompt completion of a new, strengthened framework will meet this objective and cut through the uncertainty and multiplicity of issues to be resolved. If completion is delayed, however, companies, DPAs, and data subjects all may find themselves burdened by unnecessary changes as a result of legal regimes that are moving targets.

As the Commission recognized following the Court decision, transatlantic data flows should not cease in response to the decision. It is therefore vital that the Commission and Working Party act to sustain these essential data flows by

[1] Working Party on the Protections of Individuals with regard to The Processing of Personal Data, First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy (XV D/5020/97-EN final WP4)(26 June 1997).

recognizing explicitly (as both Mme. Falque-Pierrotin and the UK Information Commissioner have done) that a transition to a new basis for these vital data flows will take time. In particular, we note that under Directive 95/46/EC that there was a transitional period of three years for EU Member States and therefore, in effect for companies to implement the requirements under the Directive. The Commission took time beyond these three years to establish a regime to address ongoing data flows, which addressed not only those to the United States through the Safe Harbor Framework but also to other third countries including later-admitted members of the EU.

A comparative adequacy assessment of the legal orders in the EU and US will be needed in numerous cases. Therefore, the Working Party and the Commission should work together to conduct a comparison of the legal orders and practices in the United States and European Union member states with regard to government surveillance and enforcement of privacy and data protection rights. Such a coordinated comparison would assist national data protection authorities, ensure adequate resources for a thorough examination of the laws in force, and avoid duplication of effort, inconsistent outcomes, and misunderstandings that would work against a single market.

It is important to recognize that the principles incorporated into the 2000 Safe Harbor Framework are those of Directive 95/46/EC and that companies subscribing to the Framework are legally bound to practices that are consistent with European data protection. While the *Schrems* decision found that the Framework did not undertake to address limits on the scope of U.S. surveillance, it did not call into question the Safe Harbor principles themselves. It is proportionate and in the interests of European data subjects to maintain adherence to these principles until alternative mechanisms are certainly and finally in place and companies are able to adjust accordingly.

In acknowledging the need for an adjustment period while the Commission, data protection authorities, companies, and civil society evaluate government surveillance laws and new data transfer mechanisms, therefore, the Commission and Working Party should acknowledge the continuing force of the Safe Harbor principles, in combination with robust enforcement by the US Federal Trade Commission, in providing a high level of data protection for EU citizens during the adjustment period.

Companies would like to move as quickly as possible to adjust to the change brought about by the CJEU's *Schrems* decision. However, uncertainty and complexity leave it unclear in what direction they should move. Decisions by the Commission and Working Party lie in the critical path to decisions and actions by companies.

Accordingly, the Commission and Working Party should take immediate steps to cut through the uncertainty and complexity and allow a period of adjustment to maintain continuity of transatlantic data flows while allowing for orderly transitions to new grounds for these data flows.

Respectfully submitted,

Jacques Bourgeois
Senior Advisor

Cameron F. Kerry
Senior Counsel

Addressees and copies attached

Mr. Frans Timmermans
First Vice-President,
Commissioner for Law and the
Charter of Fundamental Rights
Secretariat Article 29 Working Party
European Commission
Avenue du Bourget no. 1
1140 Evere, Belgium

Ms. Vera Jourová
Commissioner for Justice, Consumers and
Gender Equality
European Commission
Secretariat Article 29 Working Party
Avenue du Bourget no. 1
1140 Evere, Belgium

Mme. Isabelle Falque-Pierrotin
Chair, Article 29 Working Party
European Commission
Avenue du Bourget no. 1
1140 Evere, Belgium

Sig. Giovanni Buttarelli
European Data Protection Supervisor
Rue Montoyer 30
Brussels, Belgium

Cc:

Michelle Sutton, Cabinet of VP Timmermans
Bernd Martenczuk, Cabinet of VP Timmermans
Liene Balta, Cabinet of VP Timmermans
Renate Nikolay, Cabinet of Commissioner Jourova
Kevin O'Connell, Cabinet of Commissioner Jourova
Bruno Gencarelli, DG-Justice
Member State National Data Protection Authorities