S.C.O.P.E.
for
Transatlantic eDiscovery

resolution economics LLC

March 1, 2018

resolution economics LLC

S.C.O.P.E. FOR TRANSATLANTIC eDISCOVERY

A Framework for Considering and Obliging Fundamental Data Privacy Rights Under GDPR

BY
COREY E. GILDART

Beginning May 25, 2018, the General Data Protection Regulation (GDPR) shall serve as the centralized legal instrument protecting the Personal Data[i] of European Union (EU) citizens from privacy and data breach. GDPR protections and remedies are intended and necessary so that Personal Data may move as freely[ii] within the EU as the citizens therein. The Regulation thus concentrates considerably on Personal Data transfer between national authorities of Member States. This poses a myriad of interpretive issues, especially for cross-border eDiscovery working groups outside of the EU, not the least of which is the distribution of responsibility and liability[iii] between U.S. data processing vendors and the global client organizations through whom they work.

The EU – U.S. Privacy Shield principles attempt to proactively alleviate the imprecise application of GDPR for U.S. entities but there is no certainty that this program will suffice over the long-term. It is therefore incumbent upon all anticipated actors, both actual and ostensible, to be mindful of the core GDPR principles of lawfulness, fairness and transparency[iv] when preparing and executing transatlantic data transfers.

ORIGIN

In 1995, The Data Protection Directive provided Member States three years from the date of adoption to independently enact laws, regulations and administrative support processes to comply with the Directive and protect the fundamental right to privacy.[v] The resulting laws created a decentralized but baseline program of enforcement to enable the free movement of data between Member States. The Directive further allowed the transfer and subsequent processing of Personal Data to third countries outside of the community where the country of the receiving party also provided an "adequate level of protection."[vi] Unfortunately, the U.S. lacked and still lacks the requisite adequacy.

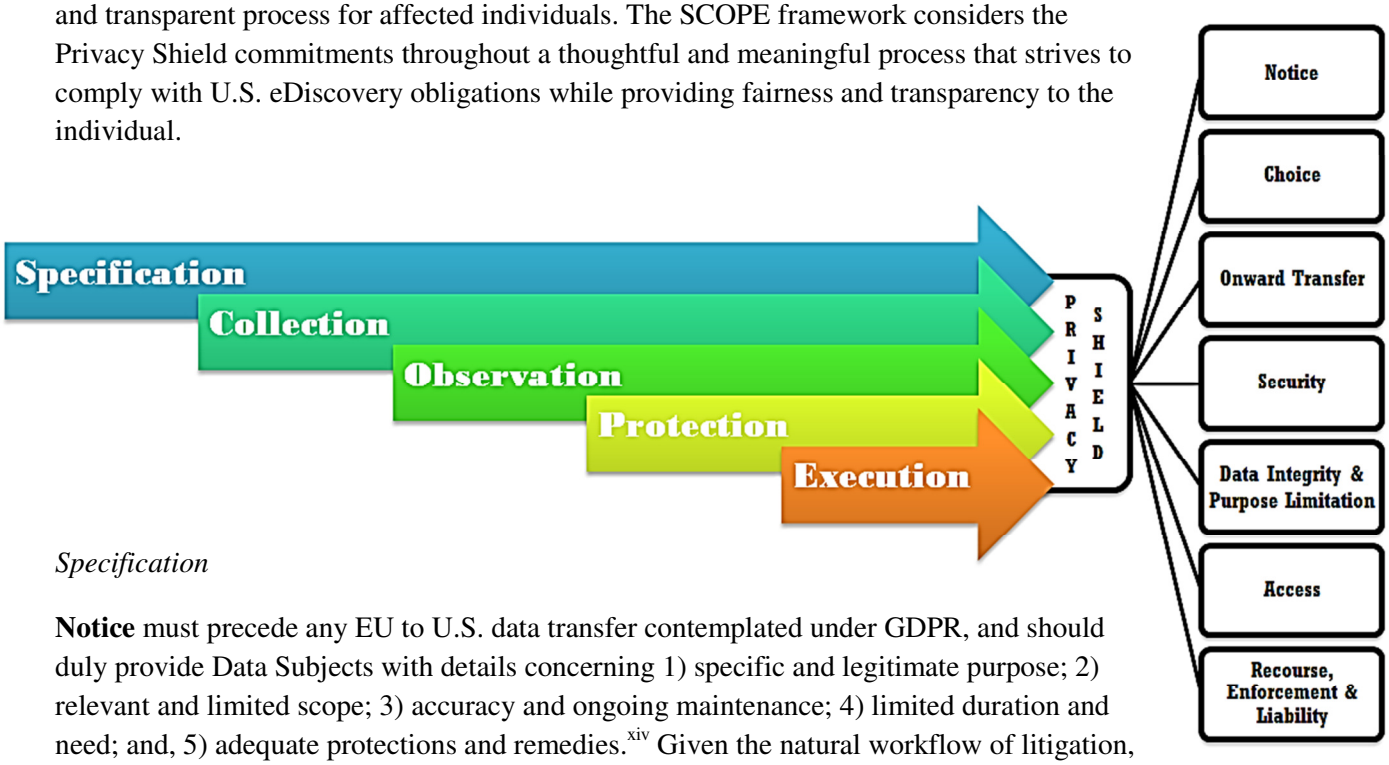
U.S. entities largely relied on Standard Contractual Clauses ("SCC's") until the Safe Harbor Privacy Principles enabled U.S. organizations to independently comply with the Directive's principles starting in 2000.[vii] The Court of Justice of the EU (ECJ) invalidated the Safe Harbor agreement in 2015 because the agreement could be actively circumvented by U.S. public authorities to the extent necessary to meet national security needs. The ECJ also expressed apprehension about the lack of remedy and recourse for the individual.[viii]

Many U.S.-based companies have reverted to SCC's in the interim to facilitate ongoing transatlantic data flows;[ix] however, GDPR will reduce the long-term viability of boiler plate SCC's.[x] A proactive mechanism for continued transatlantic data transfers under GDPR has thus been implemented as a successor to Safe Harbor. This is Privacy Shield.

The Privacy Shield program and its principles are not law per se but a quasi-contractual set of organizational commitments enforced by the U.S. Department of Commerce: 1) Notice; 2) Choice; 3) Onward Transfer; 4) Security; 5) Data Integrity & Purpose Limitation; 6) Access; and 7) Recourse, Enforcement & Liability.[xi] The commitments are insufficient without an understanding of and intent to directly comply with GDPR's own unambiguous and principled requirements that enhance the legal focus more strongly on the individual's rights and inclusion in the Personal Data transfer process. The question becomes one of process. How does an eDiscovery working group reconcile its Privacy Shield commitments with a process that is GDPR aware?

SCOPE

Processing data in a non-GDPR approved third country shall be lawful where the Data Subject[xii] has given consent or where processing is necessary for compliance with a legal obligation to which the controller is subject. [xiii] One could argue, quite unsuccessfully, that the lawfulness of eDiscovery under GDPR is a foregone conclusion, particularly where the transferring organization is a plaintiff to U.S. legal proceedings. A plaintiff, as it would be, initiated U.S. discovery obligations by virtue of a complaint and should comply therewith. But EU organizations typically underestimate the breadth and impact of highly transparent U.S. discovery rules on the individual and organization alike, necessitating a fair and transparent process for affected individuals. The SCOPE framework considers the Privacy Shield commitments throughout a thoughtful and meaningful process that strives to comply with U.S. eDiscovery obligations while providing fairness and transparency to the individual.



Specification

Notice must precede any EU to U.S. data transfer contemplated under GDPR, and should duly provide Data Subjects with details concerning 1) specific and legitimate purpose; 2) relevant and limited scope; 3) accuracy and ongoing maintenance; 4) limited duration and need; and, 5) adequate protections and remedies.[xiv] Given the natural workflow of litigation, an obvious moment for providing notice would be at the time of legal hold notification; though, the traditionally broad preservation notice would be insufficient. These are very precise requirements and demand clear specifications. Consequently, an eDiscovery working group should work to create specifications for the project before engaging in collections and transfer.

Certain details may be elusive depending on the underlying subject matter but a preliminary assessment should always start with identification of the primary Data Subjects – individuals directly scrutinized or

contemplated in the proceedings, often referred to as the custodians for collection. Secondary Data Subjects that knowingly interact with the primary Data Subjects should also be considered, particularly those that are part of the same organization or party. These are likely the individuals that require notice.

Additional analysis should include the anticipated data types to be collected, such as e-mail, audio and video, and whether the expected content contains Personal or Sensitive Data[xv] to a consistent and identifiable degree. Clearly defining the objective and subjective, for lack of a better term, scope of the project will adequately inform the working group as well as the Data Subjects as to the notice requirements outlined above, and should be amended as new information is aggregated throughout the workflow. Moreover, a clear and precise specification will alleviate any concerns from opposing parties.

Collection

Data collections may commence upon completion of a specific scope and proper notification thereof. But collections, like all of the SCOPE process, should be thoughtful. It is recommended that collections are conducted within the boundaries of the EU, even if executed remotely within the community, and preferably by and at the direction of EU citizens. This mitigates the collecting party's risk profile[xvi] during the early phases of the eDiscovery lifecycle.

Oftentimes, the collections personnel are both internal and external to the transferring client organization. The working group must therefore consider each party that will control the data and provide Data Subjects with **Choice** as to whether the subject Personal Data may be transferred to a third party where the third party is not a contractually obliged agent of the Controller or whether the subject Personal Data may be utilized in a manner outside of the originally conveyed and intended purpose.

Observation

Privacy Shield requires that actors only process such data for the limited and specific purposes, and provide adequate protections.[xvii] Observational fact-finding to confirm and refine the original project specifications will further inform pre-transfer culling and protection protocols. The assessment may also identify unanticipated Personal Data contained in the collection, e.g. tertiary Data Subjects, and expand the notice pool. The further removed identifiable Personal Data is from the limited and intended purpose, the more aggressive the protection measures and the more transparent the process must be for Data Subjects, particularly during any **Onward Transfer**.

Protection

An organization must take reasonable and appropriate **Security** measures to protect from loss, misuse and authorized access, disclosure, alteration and destruction.[xviii] Controllers commit to **Purpose Limitation** in furtherance of this effort. The working group should therefore cull irrelevant data pre-transfer. Proactive redaction can further limit accessibility to certain unrelated Personal Data contained in otherwise relevant documents. Tools such as Mylili's Blackout are able to use standard text inputs to mass redact irrelevant Personal Data, and should be considered both pre- and post-transfer. Similarly, audio redaction and facial blurring should be carefully considered throughout the eDiscovery protocol.

Execution

Executing the actual transfer and subsequent processing of only relevant Personal Data in the U.S. is feasible for most eDiscovery providers. Execution, however, extends beyond the technical cross-border transaction and requires ongoing surveillance and maintenance. Processors, for instance, must be in a position to promptly provide **Access** to Data Subjects for validation of **Data Integrity**. Privacy Shield participants further provide Data Subjects with legal methods for **Recourse, Enforcement & Liability.** Although many of these Privacy Shield commitments are addressed somewhat linearly herein, parties to a transatlantic Personal Data transfer need to remain cognizant of the overlapping principles throughout the SCOPE workflow. Fairness and risk mitigation will ultimately be achieved through inclusion. It is an imperfect process but a measure of meaningful eDiscovery management will not only ensure technical compliance but also lawfulness, fairness and transparency in accordance with the underlying data privacy obligation.

---

[i] "'[P]ersonal data means' any information relating to an identified or identifiable natural person […] such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[.]" The General Data Protection Regulation. [2016] O.J. L 119/33, at art. 4(1) [hereinafter GDPR].

[ii] "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime." Consolidated Version of The Treaty on the European Union. [2016] O.J. C 202/01, at art. 3(2).

[iii] Presumably, everyone will be jointly and severally liable for any infractions. See GDPR, *supra* note i, art. 82(4), at 81.

[iv] *Id*. art. 5(1)(a), at 35.

[v] Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. L 281/31 at art. 32 [hereinafter The Data Protection Directive].

[vi] The Data Protection Directive, *supra* note v, art. 25, at 45.

[vii] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. 2000 O.J. L 215/7.

[viii] Maximillian Schrems v Data Protection Commissioner (Schrems I), Case C-362/14, [2015] EUECJ, ¶ 22 & 95.

[ix] The Data Protection Directive, *supra* note v, art. 26(1), at 46.

[x] Entities may potentially get approval of binding corporate rules from the supervisory authority. See GDPR, *supra* note i, art. 47, at 62-64.

[xi] The Commission shall take appropriate steps to develop international cooperation mechanisms to facilitate the effective enforcement of legislations for the protection of Personal Data. *Id*. art. 50(a), at 65.

[xii] A Data Subject is "[A]n identifiable natural person […] who can be identified, directly or indirectly, in particular by reference to an identifier." *Id*. art. 4(1), at 33.

[xiii] Processing in a third country, in the absence of an adequacy decision shall be lawful where the data subject has given consent or where process is necessary for compliance with a legal obligation to which the controller is subject, see *Id*. art. 49(1)(a) & (c), at 64.

[xiv] *Id*. art. 5, at 35.

[xv] "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." *Id*. art. 9(1), at 38.

[xvi] For example, "Infringements [of Articles 5, 6, 7, 9, 12 to 22, 44 to 49, 58(1) or 58(2), or Chapter IX] shall […] be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[.]" *Id*. art. 83(5), at 83.

[xvii] *Id*. art. 25(2), at 48.

[xviii] *Id*. art. 32, at 51-52.