BRC
BOARD RISK COMMITTEE
BOARD RISK REPORT

October 18, 2021

Balancing Data Privacy with Data Transfers: A Board Member's Guide

By Kabir Barday

In July 2020, the EU Court of Justice's (CJEU's) Schrems II judgment invalidated the EU-US Privacy Shield and required additional safeguards when using standard contractual clauses (SCCs) to transfer personal data from the European Union (EU) to outside jurisdictions. As a result, many organizations had to (1) find supplementary measures to fill gaps in data protection and lawfully transfer personal data and (2) evaluate the level of data protection in third countries. Since then, organizations have eagerly waited for the European Data Protection Board (EDPB) to provide clarity in its final Schrems II recommendations on supplementary measures for international personal data transfers. On June 18th, the EDPB released that guidance, and now boards should be prepared to make sure that the organizations they oversee demonstrate compliance.

The Schrems II decision has changed the way companies importing and exporting data from the EU will work with third parties.

The Schrems II judgement established new requirements for any business transferring data to third parties from the EU. A key requirement is to ensure that a recipient third party/country can provide an essentially equivalent ('European Essential Guarantees' / 'EEGs') level of protection for personal data. Many organizations will find that standard to be a significant reach.

This EU Court's judgement reinforced the importance of data governance. As a first order of business, board members should ensure that the organizations they serve have a reasonably robust data governance scheme and that it is appropriately resourced.

In order to understand whether EU equivalent protection can be maintained over time, data exporters, in collaboration with data importers, are expected to conduct periodic assessments of relevant legislation and practices in jurisdictions outside of the EU.

Practically speaking, the ask from U.S. based businesses is high, and European regulators have signaled that while they are immediately enforcing these new obligations (see German and Spanish Data Protection Authorities' enforcement activity regarding data transfer risk assessments), they are primarily asking businesses to show clearly outlined process and evidence of data transfer compliance.

The Schrems II decision was made specifically against the backdrop of United States' rule of law. Because data transfers between the EU and the US remain a top priority, boards should ensure their organizations have adequate processes in place to protect themselves against legal action.

Questions Boards Should Consider:

- How does the Schrems II decision impact the way your organization imports or exports data out of the EU?
- Does your organization have processes in place to assess a third-country's level of personal data protection?
- Does your organization have a proactive, risk-based approach for third-party data transfers?

Organizations must evaluate and adopt supplementary measures for personal data transfers whether they import or export data.

In today's Schrems II environment, many organizations are looking for a one size fits all, "perfect" combination of supplementary measures they can take to meet and exceed new data transfer expectations. That universal combination does not exist. For every organization and every transfer, a unique mixture of technical, organizational, and contractual safeguards will be appropriate. That said, organizations are also realizing that there are sets of high-risk data transfers where available measures are simply not "good enough" and, as a result, data transfers to certain vendors and/or countries may not be permitted.

Organizations have a specific set of obligations as data importers. They must:

- Adhere to the agreed supplementary measures as well as any other applied measures to protect the transferred personal data.
- Notify exporters in cases where the importer (or its vendor chain) is unable to comply with the measures in a data protection agreement or Standard Contractual Clauses (SCCs).
- Notify data exporters when a change in the applicable legislation is likely to negatively affect the capacity of the importer to comply with its obligations.
- Notify all exporters in a timely manner regarding every circumstance where it is the addressee of specific requests or actions - i.e. an executive order/surveillance order in a non-EU jurisdiction.

Often, data importers have a broader contractual duty to provide information and support to the exporters regarding audits and compliance-related efforts. Examples of this include supporting customer-driven audits, sharing regular penetration test results and International Standards Organization (ISO) certification updates.

Data exporters, too, have specific obligations:

Most of an exporter's obligations are driven by the General Data Protection Regulation's (GDPR's) accountability principle – the exporters must review, *continually* re-assess, and *document* the measures they have applied to protect the data transfers. Applying the old adage of 'Trust but verify' is very helpful here.

Exporters are also in the driver's seat for the Transfer Impact Assessment (TIA), which identifies the risks when transferring data between the EU and countries, such as the US, without GDPR adequacy. These assessments also capture the measures applied to meet those risks. Exporters decide whether the combination of supplementary measures applied fits the bill for the transfer at hand and does enough to mitigate the transfer risks.

Questions Boards Should Consider:

- Has your organization effectively filled any personal data transfer compliance gaps?
- Does your organization understand its new obligations as a data importer?
- Does your organization understand its new obligations as a data exporter?

Keys to Effective and Compliant Data Transfers Under Schrems II

Showcasing your organization's ability to seamlessly collect information and assess vendors can be a differentiator to your business partners. That capability will depend upon and will, over time, strengthen your business's data governance, ethics and other environmental, social and governance (ESG) practices, all to your firm's benefit. At a time when fortifying business relationships across international boundaries is becoming more challenging, clean data transfer operations are an important signal of dedication to key underlying principles.

Management can take many actions to meet the European Data Protection Board (EDPB) Guidelines. A few top examples include:

- Mapping data transfers,
- Understanding and prioritizing which vendors/assets carry the highest risks due to the factors involved (e.g. types of PII transferred, countries involved, entities/jurisdictions in scope etc.),
- For each high-risk vendor, operationalizing completion of the transfer risk assessment through both internal external due diligence,
- Setting up standardized vendor transfer risk management process – applying company-approved supplementary measures for vendors and establishing acceptable risk levels for each transfer.

One of the best ways to take on the obligations relating to data transfers is to leverage vendor vetting processes already in place.

Additionally, the Schrems II decision can be a great catalyst to upgrade your program beyond minimum compliance standards. Many privacy laws such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR) are already prompting companies to explore broader principles of transparency, data minimization, and privacy by design. As a result, these companies are one step closer to tying their vendor review together with questions relating to the businesses' sustainability efforts, ethics, social responsibility, and other key factors that help drive the industry forward and are increasingly becoming a competitive advantage.

Questions Boards Should Consider:

- What steps is your organization taking to ensure compliance with EDPB guidelines?
- Is your organization evaluating vendors in a way that is leverageable to help meet or exceed Schrems II data transfer compliance?
- Is your organization's ability to vet vendor's data governance practices being positioned as a competitive differentiator?

RECOMMENDED RESOURCES

- **Webinar**: Prepare for the Schrems II September Deadline
- **Infographic**: Global Data Transfer Mechanisms Infographic
- **Webinar**: [Privacy Panel] Managing Vendors: New Compliance Considerations, Essential Assessment Techniques, and Contracting Best Practices
- **Blog**: The Definitive Guide to Schrems II

ABOUT THE AUTHOR

Kabir Barday
Founder, President, and CEO, OneTrust

Kabir is the Founder, President, and CEO of OneTrust. In five years, Kabir has grown the company into the #1 fastest growing company on the 2020 Inc. 500 and category-defining enterprise technology platform to operationalize trust. According to TCV, OneTrust is the fastest growing enterprise software company in history. OneTrust has largely pioneered the trust technology market, has been awarded 150 patents, and acquired 8 companies along the way.

OneTrust's mission is simple: Use technology to help organizations be more trusted, and turn trust into a competitive advantage. OneTrust has developed a Trust Cloud platform that helps organizations embed privacy, security, data governance, ethics, GRC, and ESG into their culture and operations. Today, OneTrust is used by more than 10,000 companies, both big and small, including over half of the Fortune 500. OneTrust employs 2,000 people in 13 global offices across North America, South America, Asia, Europe, and Australia.

OneTrust has raised $920 million funding round a $5.3 billion valuation from investors Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, and Franklin Templeton.

UPCOMING EVENT

Peer Forum For Corporate Board Risk Committee Members And Chief Risk Officers
Tuesday, November 16, 2021
9:00 AM – 12:30 PM ET - Virtual Event

About the Event **Register**

Join the Board Risk Committee (BRC) for its inaugural event. With strategic partnership from BlackRock, and support from Women Corporate Directors, this virtual peer forum will launch the BRC as a trusted place for the exchange of ideas, best practices, and topics of interest. We welcome the opportunity to offer complimentary attendance to corporate board directors who sit on risk committees or audit committees who handle risk, corporate board directors who are interested in risk committees, and Chief Risk Officers.

WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

Contact:
Catherine A. Allen, Founder, Chairman, Board Risk Committee, cathy@santa-fe-group.com
Ellen Dube, Executive Director, Board Risk Committee, ellen@boardriskcommittee.org