August 5, 2020

I hope this email finds you and yours safe and healthy. This update will be distributed on an intermittent basis to help inform BDO clients about the ever-changing global privacy and data protection landscape.

CAYMAN ISLANDS

Need to know: General Data Protection Regulation (GDPR) update

The Court of Justice of the European Union (CJEU) issued, on 16th July 2020, its decision on the so-called "Schrems II" case (Facebook case) and invalidated "Privacy Shield" for data transfers. CJEU called into question the extent to which E.U. data exporters could rely on the European Commission's Standard Contractual Clauses (SCCs), which are still valid for data transfers to the United States, and globally. At the heart of this decision sits what the CJEU considers as fundamental differences between E.U. privacy law and U.S. surveillance law which makes them incompatib

The CJEU, however, reaffirmed the validity of SCCs as a data transfer mechanism under the E.U. General Data Protection Regulation (GDPR), including to the U.S, but the CJEU requires that data exporters from the E.U. and data importers from other countries to conduct competence assessment of the data importers ability to comply with the SCCs under their domestic law, specifically identify "additional safeguards", "supplementary measures" and "effective mechanisms" where necessary. The CJEU further noted that non-EU organisations importing data from the E.U. based on the SCCs must inform data exporters in the E.U. of any inability to comply with the SCCs. As a result, we continue to see a steady increase in activity from both data privacy regulators and increasing penalties for leaving data unprotected. It is this combination of accelerating the use (and processing) of Personal Identifiable Information (PII) data and the hastening use of offsite services (such as, cloud services, working from home, working remotely etc.) and growing regulatory complexity that is creating BIG challenges for companies here in Cayman and across the Caribbean region.

In summary:

1. Privacy Shield is invalidated, so it is now unlawful to legitimise data transfers to the U.S.
2. Data exporters and importers using SCC must verify the level of protection in the 3rd country first.
3. Data Protection Authorities must now focus on data transfers.

What does this actually mean?

The immediate impact of the decision is on organisations that relied on Privacy Shield as a mechanism for data transfers, who are immediately viewed as unlawful, with no grace period. The expectation from the European Data Protection Board (EDPB) is for data exporters to strictly prohibit those transfers from organisations that do not undertake an assessment of their current data flows to countries outside of the European Economic Area.

It also means that, even though the SCCs remain valid, they are not necessarily the 'go-to/easy solution' anymore.

What could you do

The first recommendation would probably be to avoid taking hasty decisions but rather take appropriate and decisive steps to confirm that data transfers under your responsibility comply with the GDPR and the judgment of the CJEU, in particular:

- **Switch from Privacy Shield to alternative safeguard mechanisms**: Where only the Privacy Shield was used to legitimise the transfer, you should take steps now to ensure coverage under another safeguard.
- **Verify the level of protection of international data flows**: Once the relevant personal data flows are identified, you should assess the safeguards that apply to data transfers, including a nuanced analysis of the local laws in the recipient country. In this respect, for data transfers to the U.S., it will be especially relevant to which extent the data recipient is subject to Section 702 Foreign Intelligence Surveillance Act and Executive Order 12333.
- **Look out for statements from DPAs**: It is likely that European Data Protection Authorities and the European Data Protection Board (EDPB) will publish statements on the legality of data transfers to certain countries on the basis of SCCs, having a particular focus on data transfers into the U.S.
- **Monitor activities on updated SCCs**: Despite the fact that the CJEU declared SCCs to be valid, it is possible that the European Commission will issue a new set of updated SCCs in order to address the risks identified by the CJEU with regard to activities of law enforcement and intelligence agencies in the U.S. It is long overdue anyway since they have not been updated since GDPR.

INTERNATIONAL PRIVACY

- **Brazil's new privacy law: What you need to know about the LGPD:** Privacy, data protection, and data security have been key issues for businesses during the first half of 2020, driven by compliance concerns and pandemic-related digitisation. These issues will become even more complex for multinational organisations during the second half of 2020 due to another landmark piece of legislation: Brazil's Personal Data Protection Law (LGPD). The LGPD is Brazil's first comprehensive data protection law. Inspired by the GDPR, the LGPD deviates from its inspiration in meaningful ways. And despite recent legislation delaying the LGPD's administrative sanctions until mid-2021, the LGPD's effective date remains in flux and could arrive as early as next month. Once effective, the LGPD provides enforcement avenues other than administrative sanctions.
- **Civil Rights Organisations Submit Rebuttal to C.A. Secretary of State Opposing California Consumer Privacy Act:** On 19th July 2020, the American Civil Liberties Union ("ACLU") and several over civil rights organisations submitted a rebuttal to the California Secretary of State over the proposed California Privacy Rights Act ("CPRA"). Civil rights organisations object to the CPRA, stating that it will reduce existing California data subject rights by empowering large businesses to implement a "pay for privacy model," charging additional fees to protect personal information. Civil rights organisations also object to the proposed CPRA enforcement model, as the law would create a new, separate enforcement authority.
- **Hellenic Data Protection Authority Fines New York College over GDPR Accountability Obligation Breach:** On 29th June, 2020, the Hellenic Data Protection Authority ("HDPA") of Greece issued a fine

of €5,000 (approx. $5,787) to the New York College S.A. over a breach of the accountability obligation under Article 5 of the E.U.'s General Data Protection Regulation ("GDPR"). The HDPA's decision (available only in Greek) ruled that the school directly contacted a complainant about an education program and subsequently failed to adequately respond to the complainant's request to access their personal data. The HDPA deemed New York College to be a data controller and noted that the school failed to demonstrate that it processed the complainant's personal data in a transparent manner. In addition to the fine, the HDPA ordered New York College to bring their processing activities in compliance with the GDPR.

- **U.K. Government Admits to Failure to Conduct DPIA Prior to Deploying COVID-19 Contact Tracing Program:** On 15th July 2020, the U.K. government admitted in a letter to the Open Rights Group that it had failed to complete a Data Protection Impact Assessment ("DPIA") prior to the commencement of the U.K. National Health Services COVID-19 Test & Trace Program. The U.K. government noted that a DPIA is in progress and currently being finalised with the cooperation of the Information Commissioner's Office ("ICO"). The government cited the unprecedented urgency to implement such a program and noted that while the DPIA is still in progress this "should not be equated with a failure to ensure that the protection of personal data has been an important part of the program's design and implementation."

COMMENTS OR QUESTIONS? CONTACT:

Richard Carty
Risk Advisory Services – Data Privacy & Protection

+ 1345 815 4548 / rcarty@bdo.ky

Glen Trenouth
Risk Advisory Services - Data Privacy & Compliance

+1 345 815 4511 / GTrenouth@BDO.KY

This information has been collected through a number of sources including but not limited to BDO's public research, research using BDO's One Trust Data Guidance subscription, and the International Association of Privacy Professionals. Complimentary updates will be sent to our clients until August 5, 2020.