POST GDPR WORLD – CROSS-BORDER DATA PRIVACY BEST LINE OF DEFENSE

Organizations operating internationally should become aware of the best line of defense on data privacy and avoid the increasingly genuine risk of penalties associated with personal privacy law violations.

GDPR, as well as other regulations on data privacy, are more restrictive than ever before, increasing the challenges of transferring data for defending against allegations of corruption. The eDiscovery required to get the information needed in a compliant way to respond to investigations is taking on a great deal more complexity and risk. Since implementation of the new regulation, European Regulators are intensifying GDPR enforcement. This was evident when a number of organizations were targeted in the first six months of this year, including Facebook. The first enforcement action has been taken by the UK’s data protection authority (ICO) against AggregateIQ Data Services Ltd, a data controller outside the European Union. The notice is related to the processing of UK and EU citizens’ personal data for Brexit campaigns. The ICO has threatened to fine AggregateIQ up to 4 per cent of annual worldwide turnover or €20 million (whichever is greater) if they do not comply.

These warnings, investigations and enforcements demonstrate the potential for enforcement under the GDPR against companies in and outside of the EU.

HOW TO MANAGE CONFLICTS OF LAW IN A GLOBAL INVESTIGATION POST GDPR

There were significant developments in data privacy regulation leading up to the GDPR including the repeal of Safe Harbor; Introduction of the EU-US Privacy Shield and Swiss-US Privacy Shield; UK data privacy issues with the unknown Brexit status; and the election of Donald Trump all of which resulted in many stakeholders scrambling to prepare for the new regulation. The GDPR represents the crystallization of the fundamental differences between US attitudes and regulation in respect of data privacy (the antiquated US Privacy Act was drafted in 1974, since which time Europe has rewritten its privacy rules three times), and those held dear and now enacted by the European Commission (EC) in Europe. Now that GDPR has been in full effect since May 2018, it is critical for international corporations to address data transfer issues related to cross border litigation and investigations.

WHAT’S HAPPENING?

GDPR has now officially replaced the Data Protection Directive 95/46/EC (the “Directive”). The new regulation differs from the Directive on data privacy and data transfer in that the focus is now on accountability (as opposed to the old directive which was based on notification requirements). This is clearly evidenced by the ongoing investigations and notices being served worldwide. Responsibility not only falls on a “data controller” but also a “data processor” – so eDiscovery consultants are held accountable as well. This means that the data controllers and data processors must implement technical and organisational measures, as well as demonstrate compliance when it comes to handling data that may cross multiple jurisdictions under the GDPR.
WHAT ARE THE CHANGES?

GDPR preserves the core principles and the Adequacy Criteria of the Directive but aims to simplify the process for methods of cross-border transfer of data and aims to ensure security. There are many new obligations (some listed below) under the GDPR which require companies handling EU citizens’ data to undertake major operational reform.

- **Code of Conduct** – the GDPR endorses the use of codes of conduct and certifications to demonstrate compliance.
- **Extra Territorial Reach** – the territorial applicability under the GDPR is clear in that it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. Further, it applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU and non-EU businesses conducting processing activities of EU citizens, the appointment of a representative within the EU.
- **Consent** – the conditions for consent to process data have been strengthened and must be intelligible. And, a data's subject's consent to process their personal data is required to be as easily withdrawn as it is granted.
- **Breach Notification** – the GDPR contains a definition of “personal data breach,” and notification requirements of less than 72 hours to the supervisory authority.
- **Right to Access** – individuals will have the right to access their personal data so that they are aware of and can verify the lawfulness of the data processing. The data controller must provide a copy of the personal data, free of charge.
- **Right to be Forgotten** – is the right for individuals to request the deletion or removal of personal data when there is no compelling reason for its continued processing.
- **Appointment of Data Protection Officers (DPOs)** – currently, data controllers are required to notify local Data Protection Authorities (DPAs) of any data processing activities. Under the GDPR, DPO appointment will be mandatory for controllers and processors whose core activities consist of processing operations.

WHAT TO DO IN A POST-GDPR WORLD?

For industry practitioners and companies involved in investigations or expecting regulatory probes or even cross border litigation, there is no single solution to protect a company against violation of data privacy regulations around the world, but understanding GDPR in the context of a cross-border investigation, and in particular the process of eDiscovery, can help organizations contain an investigation and prevent criminal violations. As specialist consultants in trans-jurisdictional data privacy and data transfer, we recommend a few measures that can be undertaken to mitigate risks include:

- **Data governance** – knowing what data is being considered; the jurisdiction where the data resides; applicable data privacy regulations; and what clearance is required.
- **Collection and preservation** – ensure that appropriate risk management tools have been engaged and steps have been taken to ensure compliance with data regulations and the jurisdictional source of any relevant data.
- **Training and escalation** – up-to-date training regarding transfer protocols and jurisdictional data privacy regulations for all personnel involved in investigations and data transfers.
- **Data transfer strategy** – a strategy that takes into consideration the nature of the data, its origin, data privacy and other data-related constraints.
BEST METHODS OF DATA TRANSFER

• **Individual Consent** – a data subject gives consent to transfer. This is the simplest method, but can present impracticalities and as such requires careful consideration.

• **Binding Corporate Rules (BCRs)** – are a set of rigorous rules based on European data protection standards that require completion of an application and approval of DPAs. Approved BCRs permit the flow of data within the defined corporate group, no matter where the entities are located.

• **Standard Contractual Clauses** – also referred to as Model Contracts – SCCs are sets of contract clauses that were issued by the European Commission for purposes of establishing safeguards to allow for the transfer of personal data from the EU to non-EU countries (such as the US).

• **Mutual Legal Assistance Treaty (MLAT)** – an agreement between countries to share information – note that this is specifically addressed in Article 48 of the GDPR.

• **Privacy Shield** – a framework designed by US Department of Commerce and the European Commission and Swiss Administration to facilitate transfer of personal data from the EU and Switzerland to the US. This framework still remains untested in court and is potentially vulnerable to legal challenges. Moreover the uncertainty around the Privacy Shield is compounded by the potential impact of Trump’s wide Executive Order which both potentially limits data protection rights of non-US citizens and could see US government agencies insisting on access to European citizens’ personal data, having met a very low threshold of proof – a mere “risk to public safety”.

Strategic decisions regarding data made today in litigation or investigation may be subject to enforcement. Companies and their counsel collecting data as part of an investigation or litigation should consult and involve an expert eDiscovery consultant who is well versed in cross-border data privacy and transfer from the outset in any cross-jurisdictional investigations to avoid considerable penalties in the future.

ABOUT FRA

We offer extensive multi-jurisdictional data privacy, transfer, and protection expertise in order to assist our clients achieve their objectives with compliance, litigation and investigations. We ensure the highest levels of data security through global regulatory compliance with such laws as Clarifying Lawful Overseas Use of Data Act (CLOUD Act), General Data Protection Regulation (GDPR), blocking statutes and banking secrecy.

Our full-service Mobile Discovery Solution offers a scalable end-to-end mobile processing and review platform capable of handling complex project requirements and can be installed on-site independently or in a client infrastructure anywhere in the world. For the highest levels of data security, our mobile discovery solution can be air-gapped to restrict any outside access.

Download our eDiscovery Consulting differentiators

UK | US | France | Switzerland | Finland | Canada

www.forensicrisk.com