The Question of Data Sovereignty and the Influence of GDPR

Stricter data sovereignty laws could raise new geopolitical barriers and may encourage asset managers to safeguard client data at home

The storage and transfer of client data across borders within the European Union (EU) will be a key challenge for investment firms as they look to comply with reporting obligations under MiFID II. As Member States move to draft stricter data residency and sovereignty laws to protect citizens' privacy, asset managers will need to be more vigilant about the security and location of their clients' personal information.

Privacy concerns fueling stricter protections

'Data sovereignty' describes the concept that data stored in a digital form falls within the legal jurisdiction of the country in which it is stored. With increased global connectedness and the use of cloud computing, compliance with data sovereignty rules has become more challenging. Firms will need to devote more attention towards how their clients' data is stored and transferred in the cloud as service providers often maintain operations and facilities in third countries to reduce costs and maximize economies of scale.

GDPR to impose stricter data protection standards

The challenge for firms to manage rising data sovereignty is increased due to different approaches by governments to ensure the privacy of citizens' data. Some of these concerns will be addressed under the new General Data Protection Regulation (GDPR), which will harmonize data legislation across the EU after its implementation on May 25, 2018.

However, the new legislation will also impose tougher data protection standards on investment firms that, under MiFID II, must hold more data about customer transactions than ever before.[1] Managing the requirements of both MiFID II and GDPR could prove a delicate balance. The storage of voice recordings, for example, is one area where the regulations merge. MiFID II stipulates that all voice recordings should be kept for five years minimum, while GDPR states in a more generic fashion that they should not be kept for longer than needed.[2] However, the GDPR further indicates that that the duration of the storage may be defined by other applicable regulations, such as MiFID II.

The GDPR will also place stricter standards on firms domiciled in non-EU countries that manage EU citizens' private data, expanding the scope of data protection rules to regulate non-EU data controllers and processors.[3] The broader scope will mean any firms that are involved in data processing activities relating to the offering of investment services to individuals in the EU, or who monitor the behaviour of individuals, may be held to account by the legislation. Non-EU investment managers that control or process personal data of EU employees or investors may therefore be within the scope of the GDPR and need to appoint a Data Protection Officer

> With increased global connectedness and the use of cloud computing, compliance with data sovereignty rules has become more challenging

KEY INSIGHTS

- New data sovereignty laws may prompt asset managers to keep clients' data within home borders
- GDPR legislation to broaden the scope of data protection rules to regulate non-EU data processors and controllers
- The vulnerability of the EU-US Privacy Shield could complicate investment managers' compliance efforts in data security and reporting

within the EU for GDPR compliance purposes. [4] The GDPR will also impose new requirements on firms relating to the analysis and documentation of data processing. The requirements will include more explicit obligations on controllers to communicate with clients as to how they process their personal data, and what their rights are in relation to that processing.[5]

EU-US data accord on shaky ground

With its wide mandate, the GDPR is seen setting standards for non-EU jurisdictions and particularly for US based companies, given that about 90 percent of European personal data is processed by US service providers.[6] Data transfer mechanisms between the EU and the US, however, may need to be addressed further.

Since the European Court of Justice struck down the 'Safe Harbour' agreement at the end of 2015, the EU-US Privacy Shield has governed transatlantic data flows. Some 2,400 companies use the Privacy Shield to certify their compliance with EU-approved privacy principles but officials have cast doubt on its suitability as a long-term instrument. “Something more robust needs to be conceived," European Data Protection Supervisor Giovanni Butterelli said in August 2017.[7] While demanding a higher level of compliance than 'Safe Harbour,' some critics believe the Privacy Shield could be vulnerable to further court challenges.[8]

Data transfer mechanisms between the EU and the US, however, may need to be addressed further

Investment managers need comprehensive review of data systems

Given that data transfers to non-EU jurisdictions are generally prohibited unless destination countries can ensure adequate protection for personal data, the lack of an agreed framework between the US and the EU could complicate investment managers' compliance efforts in data security and reporting.[9] Firms will need to factor in this risk when assessing their approach to data protection between now and when the GDPR legislation comes into force. They will also need to be mindful that service providers operating in foreign jurisdictions with weaker data protection laws may be at a higher risk of being pressured to surrender data to national authorities, as has happened to US firms controlling the data of EU citizens in the past.[10] Some firms may ultimately decide the risks are too great and elect to bring much, if not all, of their clients' data in-country rather than be exposed.[11]

Before reaching that decision, asset managers will need to undertake an exhaustive review of their data systems and service providers to ensure they have full insight into investor data flows. To safeguard client privacy when processing their personal data, firms will also need to review their notifications, processing agreements, and transfer and security arrangements.[12]

Asset managers will inevitably need to commit time and resources to meet rising data sovereignty requirements. The failure to safeguard clients' data, however, is likely to extract a far greater cost.

1. FTSE Global Markets (February 3, 2017) Seven Things You Need to Know About MiFID II and GDPR 2. ibid 3. Diginomica (April 27, 2017) The Four Pillars Of Data Sovereignty Wisdom 4. Actiance (January, 2017) GDPR Compliance and Its Impact on Security and Data Protection Programs 5. Matheson (May, 2017) - GDPR in Context: Impacts on the Asset Management Industry 6. Ibid. 7. OpenGov (August 25, 2017) Oh Data Where Art Thou 8. The Irish Times (September 7, 2017) Privacy Shield is Already Coming Apart at the Seams 9. Ibid. 10. Bloomberg (August 15, 2017) EU Court Ruling May Signal Problems for Data Privacy Shield 11. Freshfields Buckhaus Deringer (August 5, 2016) Microsoft v. United States: Court's “Privacy" Ruling Is Not Really About Privacy at All 12. CNS Group (August 16, 2016) Data Sovereignty: Keep Your Critical Data Close

12/17 17-233A