The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018, to bolster and standardize the oversight and enforcement of personal information protections. The facts and figures reveal that the law is being taken seriously by all parties. Our updated checklist can help you manage the compliance process for your due diligence application or virtual data room.

Breaches & Fines
The European Data Protection Board (EDPB) has reported that over 280,000 cases have been reported in year one.1 While there has been some criticism that fines – up to 4% of annual revenue or EUR20 million, whichever is higher – are not being imposed, data protection agencies have not been silent, with watchdogs saying the EUR56 million of fines issued so far (May 2019) is just a start.2

Risk-proofing
So, there is incentive to comply. And as a virtual data room is no longer just a storage facility for files and folders, but a place to manage your entire due diligence process – from uploading and organizing, to permitting and publishing, to analyzing and reporting – choosing a GDPR-compliant due diligence application is imperative to minimizing GDPR risks and breaches. To help you manage this process, we have provided the following checklist.

Does your due diligence application/virtual data room:

- Have independent certifications to evidence its adherence to data security?
- Provide a granular document security and robust audit trail down to the page level?
- Have a security breach response plan and team in place?
- Store customer content within the EU?
- Have valid certification under the Privacy Shield Framework for data transferred to the US?
- Carry out a regular Data Privacy Impact Assessment (DPIA)?
- Train staff to handle data in a compliant manner?
- Have overall GDPR readiness as a supplier?
- Provide the tools to encrypt/anonymize personal data?
- Provide the tools to control access to personal data?

---

1. Year GDPR- taking stock (EDPB, May 22, 2019)
2. Year 1 of GDPR (The Register, March 14, 2019)
MERRILL DATASITEONE: YOUR TRUSTED AND COMPLIANT APPLICATION FOR DUE DILIGENCE

Merrill DatasiteOne is ISO/IEC 27001 certified, SSAE 16 SOC 2 Type II attestation, and EU-US & Swiss-US Privacy Shield certified for clients with cross-border requirements.

Merrill DatasiteOne has invested in European client support and hosting facilities to maintain localisation of data in the EU under a “data trustee” agreements, where customer content is never replicated and transferred outside the EU.

Merrill DatasiteOne has an effective personal information security breach response plan in place to detect and respond swiftly to security incidents or breaches.

Merrill DatasiteOne conducts Data Privacy Impact Assessments (DPIA) on a regular basis to ensure best practices are met and industry-leading solutions are implemented where personal information is concerned.

Merrill DatasiteOne conducts mandatory Security Awareness and Data Privacy training to all employees regularly.

Merrill DatasiteOne integrated redaction, watermarking, permission staging and Q&A tools enhance data security at all stages of the due diligence process, and allow the client to always be in control of the data.

DatasiteOne, a market-leading SaaS due diligence platform, enables dealmakers around the world to focus on the deal, not the data room. Sophisticated analytics, ironclad security and world-class support make DatasiteOne the cloud-based virtual data room of choice for M&A and securities professionals in more than 170 countries.