BITSIGHT

DATA SHEET

GDPR: Managing the Risk From Processors

Monitor and regularly test third-party security performance and adherence to the GDPR

The General Data Protection Regulation (GDPR) was created for the purpose of strengthening the European Union's (EU) procedures and practices related to data protection. While the GDPR was announced in 2012 and adopted in 2016, organisations have until May 25, 2018 to become fully compliant.

KEY TAKEAWAYS:

- **Easily identify security gaps among your processors using trusted, actionable metrics.**
- **Regularly test and assess your critical processors.**
- **Align your vendor risk management strategy to the GDPR.**

THE IMPACT OF THE GDPR

The new regulation affects two different roles: **controllers** and **processors**. Both controllers (first parties) and processors (third parties) must have the appropriate technical and organisational measures to ensure that data is used only for its intended purpose and kept secure. If a controller or a processor experiences a breach, both organisations could face a maximum fine of **€20,000,000** or **4% of their worldwide revenue** (not profit), whichever is greater. Accountability now falls on both parties to proactively document — and actively manage — their compliance efforts.

BITSIGHT HELPS CONTROLLERS MANAGE RISK FROM PROCESSORS

One of the most critical requirements of GDPR is for controllers to manage cyber risk from their third party data processors. GDPR Article 32 states that controllers must enact a process for "**regularly testing**, **assessing**, and **evaluating** the effectiveness of technical and organisational measures" of third-party processors. The goal is to ensure the ongoing security of processors and their systems.

BitSight Security Ratings provide actionable data that enables controllers to test, assess, and evaluate data processors during the processor evaluation period as well as throughout the lifetime of the business relationship. This allows controllers to ensure the ongoing security of their processors with limited impact on current staffing.

BitSight Security Ratings measure the security performance of organisations on a scale of 250-900, with a higher rating indicating better security performance. BitSight Security Ratings are calculated by collecting and processing terabytes of security data collected from around the globe.

BitSight Security Ratings are automatically updated daily, allowing controllers to ensure the ongoing security of their processors by continuously tracking changes in processor security performance. Controllers can work collaboratively with processors to ensure that processor security is improved during the lifetime of the relationship. Controllers can also leverage this data during the initial evaluation process when deciding which processors to select, or during regular presentations on cyber risk or GDPR adherence to the Board of Directors.

Controllers can also uncover data processor relationships by leveraging BitSight Discover. This provides a controller with automated visibility into the many different data processors who may have access to sensitive controller data.