GDPR: WHAT TO KNOW

OBTAIN ADEQUATE CONSENT

The GDPR relies heavily an individual's consent to the use of her data in order to collect, process, store, and maintain data. That consent must be "freely given, specific, informed and unambiguous" (Art. 4(11)). Additionally, opt-out consent is no longer permitted; consent must be affirmative (i..e, opt-in).

DEMONSTRATE COMPLIANCE

The GDPR requires that the controller and processor maintain adequate records to show compliance with its requirements. This includes records of processing activities (Art. 30) and records of data impact assessments (Art. 35). These records must be produced to a Supervisory Authority within a reasonable time after a request.

VENDOR MANAGEMENT

The GDPR creates clear liabilities on both the part of the controller and the processor. Each controller is charged with ensuring that any processor of EU data provides "sufficient guarantees to implement appropriate technical and organisational measures" to meet the requirements of the GDPR (Art. 28(1).

DATA BREACH NOTIFICATION

Data security is taken into consideration in a number of ways under the GDPR. In the event of a breach, you must notify the Supervisory Authority within 72 hours (Art. 33). If that data breach is "likely to result in a high risk to the rights and freedoms of natural persons," you must notify the individuals "without undue delay" (Art. 34).

EXTRATERRITORIAL IMPACT

The GDPR applies to a company that is not established in the EU if it offers good and services to the EU or monitors the behavior of individuals in the EU (Art. 3). The GDPR requires strict adherence to cross-border data transfer mechanisms (Arts. 44-49).

ACCOUNTABILITY

The GDPR comes with very large potential administrative fines for non-compliance: the maximum fine is 20 million euros, or "4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher" (Art. 83).