GDPR THIRD PARTY RISK ASSESSMENT ONLINE PLATFORM

Has your organisation's Data Protection Officer (DPO) fully validated your compliance to GDPR? If not, consider the one area of most significant risk to your business: Third Party Data Security. A leading global certification organisation, Verego has launched a tool to address Supplier GDPR Risk.

TOP STORIES IN DATA RISK

TARGET to pay $18.5M for 2013 data breach that affected 41 million consumers – The states' investigation of the breach determined that cyber attackers gained access to Target's computer gateway served through credentials stolen from a third-party vendor in Nov. 2013"
USA Today - May 2017

AT&T data breaches exposed about 280,000 U.S. customers' names and full or partial Social Security numbers, the government said. The company agreed to pay a $25 million civil penalty to settle a Federal Communications Commission (FCC) investigation into the consumer privacy violations, the agency said Wednesday. The breaches occurred at call centers used by AT&T in Mexico, Colombia, and the Philippines when employees accessed sensitive customer data without adequate authorisation."
CNBC - April 2015

VERIZON "It is believed that as many as 14 million subscribers were impacted…These records were held on a server that was controlled by Israel based Nice Systems...an extremely well-known and trusted company that 85 of the Fortune 100 work with. In fact, Nice boasts more than 25,000 customers in more than 150 countries around the world."
Identify Force - July 2017

GDPR & 3RD PARTY RISK

The EU General Data Protection Regulation (GDPR), effective May 2018, has significant implications for personal data management for customers and suppliers. Applicable to any organisation doing business in the EU or holding personal identifiable information (PII) on an EU Citizen, GDPR applies whether or not the organisation is based in the EU. Although many organisations have an understanding of their internal data management operations, most organisations are struggling to manage, specifically in regards to the most significant risk area of GDPR: Third Party Supplier Risk.

Third party service providers are the most likely source of data breach, implicated in over 60% of all incidents. Regulators focus on the weakest link of compliance as this is where risk exposure is greatest. However, despite this significantly higher risk, third party due diligence is very often overlooked or seen as too complex.

Not only are organisations required to verify their own data processes, they will also need to validate the compliance to GDPR of their external partners. Regardless of the allocation of responsibility in supplier contracts, data subjects are entitled to enforce their rights against either the data controller or processors (e.g. subcontractors, partners, agents, suppliers, and service providers). Under GDPR, data controlling organisations and their suppliers, can be jointly individually liable for compliance to the Regulation.

GDPR THIRD PARTY RISK ASSESSMENT ONLINE PLATFORM

WHAT IS THE SOLUTION?

To address GDPR third party compliance, Verego has developed a cost effective assessment process which will allow your organisation to collect data from suppliers in a controlled fashion, provide a proof of record, assess and profile supplier risk and if necessary validate their adherence to the GDPR. The Verego process also allows suppliers to have their processes verified by an independent third party auditor. The global solution is delivered via a robust cloud based platform and is equally effective for small or large numbers of suppliers.

GDPR requires global organisations properly identify, track, and protect their EU customers' PII for both the "data controllers" and "data processors." From the buyer perspective, there is a significant chain of information necessary to identify GDPR risk and compliance for third parties, as outlined below:

- Who are the third parties handling your data?
- What are their data security procedures?
- Do you know what data they have and what are they doing with your data?
- Where is your data stored and which third parties have access?
- Do contracts include GDPR requirements for data processors and controllers?
- Has your organization done a risk assessment of your suppliers?
- Can you identify your high risk vendors?
- How do you prioritize GDPR compliance among suppliers?
- What policies, processes and technologies do they have in place related to data security?
- Have you ensured third parties can support GDPR mandates?
- Have you completed a Pre-Implementation Privacy Impact Assessment?
- Can you ascertain the GDPR awareness of all third parties with access to client or personal data?

WHAT IS THE RISK? REPUTATION+ FINES

If your organisation or one of its third parties fail to adhere to GDPR regulations resulting in the compromise of your customers' personal data, your organisation is liable.

Data security has become one of the most talked about and material corporate issues in recent years with third parties being found responsible for data or information breaches in the majority of cases.

In addition to the significant impact that the reputational damage leaks can have on a business, under the regulation fines for non-compliance, even those resulting from a third-party, can total up to 4% of annual company revenue, or €20 million, whichever is higher.

To learn more about the Verego GDPR Third Party Assessment Tool and the process of supplier data security verification, connect with **Clearstream Solutions** by contacting **brian@clearstreamsolutions.ie**