Written by Marco Attard
19 July 2018

According to Gartner, many organisations are still not compliant with GDPR legislation, even if it has been in force since May 2018-- the result of a lack of properly audited data handling within supplier relationships.

Thus, sourcing and vendor management (SVM) leaders should review all IT contracts to minimise potential financial and reputation risks.

"SVM leaders are the first line of defense for organizations whose partners and suppliers process the data of EU residents on their behalf," the analyst says. "If you don't have clarity on your organization's role with regards to personal data handling, you have to urgently address this."

GDPR points out 2 key roles-- data controllers and data processors. Data controllers are the customers of data processors in any specific activity handling the personal data of EU citizens, and the roles can change according to activity. However, if the processor is not GDPR-compliant, it can lead to penalities of up to 4% of organisation annual revenue, or €20 million.

Data processors have many requirements, including obligations to process personal data only on instructions from the controller, to inform the controller if it believes said instruction infringes on the GDPR, to notify data controllers of data breaches without undue delay and to restrict personal data transfer to a 3rd country unless legal safeguards are obtained.

Gartner has a "nonexhaustive" list for SVM leaders to set out expectations and requirements

around GDPR in contract negotiations:

- **Definitions**-- Definitions in contracts should reflect the revised definitions in the GDPR.
- **Data breaches**-- The vendor should notify in case of data breach without delay, and should cooperate, investigate and remediate the breach. It should also assit with any notifications required and work with the appropriate authorities.
- **Data security**-- Special measures such as encryption should be assessed, and "data protection by design" considered.
- **Data processing**-- Vendor data processing must allow the fulfilment of data subject requests, and all data processing activities a vendor performs should be documented.

- **Vendor cooperation**-- Vendors must support any audits the SVM (or a 3rd party on behalf of the SVM) performs to verify GDPR compliance.
- **Dealing with fines**-- The SVM must consider modifying the indemnities, limits of liabilities and other similar clauses to hold vendors accountable for noncompliance with the legislation.

"Being explicit about what you need from vendors is critical," Gartner concludes. "Moreover, it's important to explain the implications of key GDPR clauses to your stakeholders as well as to your suppliers."

Go Adjust Your Technology Procurement and Contracting Process to Avoid Stiff GDPR Noncompliance Fines