Why GDPR is much more than a client communication issue for e-commerce

While the Netherlands operates some of the most stringent data breach laws in Europe, the introduction on 25 May 2018 of the European General Data Protection Regulation (GDPR) widens the legal scope of what companies need to do to remain compliant on data protection issues. For many companies, being GDPR compliant is largely seen as a communication issue. Yet whether it’s to customers or regulators, GDPR needs to be clearly signposted within the reporting function in order to communicate explicitly on the collection and use of personal data.

We know that organizations are affected by many variables and that many companies rely on re-porting functions to capture the risks these variables present. But for e-commerce companies in particular, resolving data protection variables may call for an overhaul of reporting functions to accurately assess the risk of non-compliance. So how are e-commerce clients in the Netherlands re-acting?

Strategising internal communication

If communicating with clients in a legally compliant manner is at the heart of GDPR, then how this communication is reported needs a clear strategy. Traditional bricks and mortar operation generally have a customer facing function that is the main entry point for control and processing of data. E-commerce operations, on the other hand, engage with customers via data processing software at every stage of the online operation; from initial marketing of products or services, through to tracking, purchase and eventual fulfilment. The introduction of GDPR means clearly identifying who controls and who processes data is essential and that communication lines are designed to feed into the compliance reporting function at each step of the customer journey in order to be accurate and effective.

Assessing real-time compliance

E-commerce operations are both market and action driven. They are processing data constantly and in real time with each new and often daily marketing action leading to different data collection requirements. Such a dynamic business model makes implementing GDPR more complex as in future changes involving data need a data protection assessment. So the impact of how new mar-keting activities affect the data protection of individuals needs to be assessed. If not already in place, systems need to be able to cope with real time compliance in order to satisfy the availability of reports if a request is received from a customer or regulators.

Monitoring transparency and third party suppliers.

One of the biggest challenges for global e-commerce businesses is the difficulty of being GDPR compliant when collecting data through external parties. This is particularly important if data is sourced from a supplier in a location where data protection is not currently a legal requirement. E-commerce operations also need to tread carefully when using third party data that involves more opaque data collection functions such as customer profiling. With GDPR enshrining the rights of individuals into law, e-commerce operations will need suppliers to demonstrate how they gathered the data; what data is being processed; for what purpose and whether the customer gave consent. While tough fines will apply for non-compliance, clients need to be equally, if not more, worried about reputational business risk.

Obtaining a competitive edge

As data breaches become more common, security of data is increasingly key for clients.

Jan Matto
Partner
Mazars Netherlands

25 May 2018
The date when the GDPR comes into force

E-commerce operations that can demonstrate client data is safe will have a strong competitive edge. The ability to deliver an assurance report that you are GDPR compliant and that data collected, used and held, is both accurate and secure is becoming an increasingly important selling point when tendering for business. Of course, data required to compile assurance reports must be readily available and a format for reporting not only be in place and easily accessible, but also watertight on assurances given.

If we are to develop a true digital society, then it has to be a sustainable one. E-commerce operations are more likely to have a better chance of survival going forward if they take the opportunity to implement GDPR as a pathway to broaden reporting functions to take account of such changes.

One of the biggest challenges for global e-commerce businesses is the difficulty of being GDPR compliant when collecting data through external parties.

- Jan Matto