Cybersecurity: Can data protection regulation be an e-commerce game changer?

With 66 percent of global consumers planning on using a mobile device to make online purchases in the future, cybersecurity and data privacy risks are set to remain key challenges for e-commerce players. Additionally, a forthcoming challenge is the introduction of the EU General Data Protection Regulation (GDPR) that comes into force on 25 May 2018. It will involve e-commerce organisations implementing key changes to their systems and processes, but also altering the attitudes to the way they handle personal data in order to keep them within the legal scope. Irrespective of Brexit, companies in the UK will also need to comply now that the UK Government has introduced a bill to implement GDPR into UK national law.

Designed to harmonise data privacy laws across Europe, the GDPR gives greater protection and rights to individuals on their personal information. It also adopts a much broader view of what constitutes personal data and the way it flows in and out of organisations. As well as having to obtain clear and explicit consent from customers (clearly defining why they need to collect the individuals personal data and the way it flows in and out of organisations), organisations must be transparent with what they intend to do with the data collected. In addition, consumers also have the right to access and, to some extent, request that their data be deleted.

The GDPR has tightened its regulation belt with respect to data breaches - requiring organisations to report them within 72 hours. To avoid breaches, even e-commerce companies with a strong IT background will need to assess that their systems and processes are robust enough to comply. With only six months before the regulation comes into force, it’s becoming evident that e-commerce companies dealing with consolidation issues or legacy IT systems may struggle to comply within the timeframe. There are no easy fixes; compliance in most cases is non-negotiable. However, despite the unwavering necessity to comply with the GDPR, it can prove to be a business game changer for e-commerce companies.

1. Digital transformation

For many, the costs incurred when transforming their operations and systems in order to comply with GDPR will be a considerable amount. Nevertheless, as opposed to overhauling or beefing up existing systems and processes to simply comply, investing in innovative technology can not only enable compliance, but also improve efficiency and security. For example, the use of blockchain to encrypt transactions will mean organisations won’t need a regulatory authority or trusted third parties to ensure the security of those transactions. Furthermore, the adoption of artificial intelligence and smart wallets, puts the decision of what data is shared firmly in the hands of the customer.

2. Improve trust

The introduction of GDPR can be a facilitator to becoming more open and transparent with customers. Many organisations have used personal data to bombard customers with unwanted marketing emails and information, using the swathes of terms and conditions as a veil, hiding their true intentions of how they intend to use personal information. While it may require a change of operational culture and attitudes, raising the awareness of GDPR and going above and beyond standard requirements will result in a more transparent experience between company and customer, which will improve trust, reputation and encourage customer loyalty.

3. Business evolution

Gathering less data does not necessarily mean reduced marketing opportunities. It creates an opportunity to be smart with the data you are provided with by the customer. This should signal a move away from the e-commerce industry being reliant on gathering huge sets of data that are not well targeted or, at worst, out of date, engaging with customers on marketing preferences and fostering collaborations and new partnerships.

Of course, ensuring you have correctly interpreted how the introduction of GDPR will affect your e-commerce operations and undertaking a thorough gap analysis will be the key to highlight the necessary steps towards compliance. For companies struggling to meet the timeframe, a gap analysis can be used to prioritise key areas to focus on, usually with a risk based approach, so that the regulator can understand your compliance approach. With careful analysis and foresight, it’s an opportunity to create a more open and transparent relationship with customers, putting them back at the center of e-commerce operations. From a traditionalistic e-commerce sphere, it will be a challenge to reframe the attitudes to the way they view and process personal data, however, it should be viewed as an opportunity to re-innovate and re-connect with consumers rather than yet another regulation that needs to be complied with.


Nicolas Quairel
Global Head of Technology & Digital solutions
Mazars UK