

Will GDPR (General Data Protection Regulation) Effect the Way eCommerce Business is Done?

Not everything that happens in the world of technology and data acquisition is meant only for geeks; at times there's something for the end users as well. To find out what benefits this bonding would bring, let's first do a bit of a flashback.

For the past year and a half, there's so much going around GDPR, or General Data Protection Regulation, which is the most comprehensive data privacy law to date. The European Union's GDPR, a data protection law that passed in the EU Parliament in 2016 and which came in to force on May 25, 2018, aims to facilitate the rights of individuals to own their own data and any business handling that data must keep it secure.

The General Data Protection Regulation will mandate any company in the European Union and well as those who do business inside the EU, to adhere with strict new rules regarding the collection, storage and use of customer data. This includes all forms of customer data, such as pictures, social media posts, IP addresses, bank details, consumer history, and any numbers like an SSN, that relates to the identity of a customer. The step is to safeguard consumers from companies that may misuse their data and to help them allow and manage their data for only its intended use.

If we take a look at the impact of GDPR on eCommerce, it will cause significant change because eCommerce runs on customer data accessible on CRM, EDM, PoS and BPA systems and companies use of that data as per the needs of their business. The GDPR will now apply to all such data that is being channelized for

marketing, sales, HR, and accounting purposes. In simple words, any form of digital data that is stored or processed will fall under the new regulation and eCommerce businesses will need to comply with it.

Once implemented across all the verticals of business domains, the GDPR will empower the EU consumer to be the all-encompassing owner of their data and allow them to review, adjust, erase, and restrict the processing of their data. The consumer has to make an online request to the [eCommerce company](#) and the company will have to close the request in no longer than a months' time. In addition, if there is a need to delete any copies of personal data that is public, the companies are required to initiate a request to organizations, like Google who has already set up a process to speed things the requests.

eCommerce businesses cannot afford to make mistakes since there is so much at stake. Any infringement will attract fines of up to €20 million, or 4% of their annual revenue. Data must be stored securely and eCommerce businesses that store data using third-party software applications are solely responsible for the encryption and back up rules while protecting their customer data.

However, for eCommerce companies utilizing the cloud for data storage and access, the transition can be easy. For bigger players, significant resources will be required to become fully compliant with the regulation. The companies that rely on in-house servers or customized software solutions will require a team to assess the risks, test measures and follow processes to protect data from input to deletion.

According to the terms mentioned in the GDPR, every eCommerce company is considered the Data Controller who is responsible for the collection and safe storage of their customer data. The Data Controller will also be able to gain consent from customers and visitors to use their data in a GDPR compliant

way.

To make sure that the business is fully compliant with the regulations, the company can recruit a Data Protection Officer (DPO), integrate advanced privacy tools, evaluate data security systems, train the staff, and hire services from a third-party provider who is GDPR complaint.

If you are in an eCommerce business and serve customers in the European Union, you may now need to be concerned if your business is not GDPR compliant. We know that GDPR is giving many of us sleepless nights and a run for our money, but it is for a better future of dealing with data securely.