As a result of several billions of personal records been exposed by cyber criminals, it is no surprise that data privacy laws is an important topic right now. To counter-act this issue data privacy laws are currently being implemented with an urgency that we have never seen before. In this aspect, European Union's General Data Privacy regulation, commonly known as GDPR is known to lead as the strongest privacy and security laws in the world. According to Anastasios Gkouletsos, cybersecurity expert in a company in London, other companies who are not members of GDPR may still be non-compliant if they happen to extract data from European Union. As per his idea, in the current day universally connected environments where it is so easy to share information, it is a difficult task to remain complaint. Violations involving health, sexual orientation, race, age and weight, had many companies like Amazon Europe, WhatsApp, Google, Target, Yahoo, Marriott, Equifax, Facebook and other 900 companies being fined since GDPR law was put in place in 2016. As per Gkouletsos approximately 2% of the company's revenue incurred from these penalties fined around the world. California Consumer Privacy Act (CCPA) is another law equivalent to GDPR, which earns more $25 billion per year by collecting data around 50,000 users. This law makes sure that data in older systems cannot disregard the importance or the need for a changeable way to handle it completely. Therefore, it is really significant to adhere to privacy laws and be aware of ways on how to abide by them. Firstly, data encryption, which makes sure that it is encrypted as well as personally identifiable data removed (anonymized). Second method is cloud hosting which is adaptable by companies that are spread out geographically and therefore it is far more useful having shared environment in the cloud rather than physically hosted environments but cybersecurity and compliance standards for the cloud should be followed as appropriate. Third method is referred to as vulnerability assessments which are really penetration tests and vulnerability scans to be executed regularly using third party tools. Fourth method is applying endpoint security which is compulsory for all companies which have business locations world-wide. To manage endpoint security in an efficient manner, it is imperative that functions and components such as a firewall, malware removal, ransomware protection, device management, a password manager, patch management and a business VPN are implemented successfully. As per Gkouletsos vulnerability scan would help you to find unseen points in data security, transference and shortcomings with the help of a few vendor companies, but GDPR with its privacy security laws really keep your company secured in a consistent manner. James McQuivey, an analyst at Forrester Research, a research and advisory company based in Cambridge, Massachusetts believes that laws like GDPR would make it more difficult for that companies to figure out what type of data to collect and implement in cloud with solutions such as Oracle Advanced HCM Controls and SAP with Trust Center would provide better a solution. In contrast, cloud-based solutions would be committing unintended violations if it is placed in several locations. Some think that applications are better placed in the cloud than data because application and data both do not need to be placed in the same place. That will most probably be a better solution because the data in on-premise locations would then have better management and control. An improved version of CCPA and GDPR is called intelligent archiving, which is basically managing devices in order to perform an intelligent data movement as needed on many storage devices while adhering to data privacy laws. On top of that, a company called DataMasque has the ability to hide personally sensitive data without doing any harm to its use by applications.