PARABLU

Regulation: GDPR Accountability Principle: A change in Regulatory Landscape

If you're finding yourself walking into a hall of mirrors when it comes to GDPR compliance, don't worry, you're not alone! To begin with, if you've decided to achieve GDPR compliance, you have won the proverbial half-battle. What could help you in your journey further is understanding the core tenets of regulatory compliances and how GDPR is similar to many other regulations you may have encountered before.

All regulations, more or less, ask organizations for the same basic compliances.

1. Discover – Identify what data you have and where it resides
2. Manage – Govern how data is used and accessed
3. Protect- Establish security controls to prevent, detect and respond to data breaches or losses
4. Report – Have report and audit logs to prove you're doing all of the above.

GDPR Accountability principle: The only thing that is changing is that regulations are increasingly making organizations more and more accountable for the data they own – and that trend is unlikely to change, at least in our lifetimes. GDPR has, of course, upped the ante when it comes to making organizations pay (quite literally) for data breaches or failing to report them. GDPR expects ownership from organizations and builds cognizance into the kind of data organizations collect and process.

Trivia – A recent photo API bug on Facebook allowed third-party apps access to ‘private photos’. A bug that affected 6.8 million users. GDPR requires data breaches to be reported within 72 hours. Facebook waited two months to report the incident and came under a lot of criticism. A spokesperson of the firm stated that the delay was due to investigations that were underway, to recognize if it was a bug that had to be reported.

PARABLU

GDPR has come into the lives of IT administrators at an interesting time – a time in which there are two compelling forces shifting the data landscape. Cloud & Mobility. Even as you're reading this, data is moving out from traditional data-center silos and making its way into the cloud or is becoming resident on end-user devices. The action has undeniably shifted from the office workplace to (a) the cloud and (b) the endpoint. While the pull to the cloud makes economic sense for a lot of companies, it is counter-intuitive from a regulatory standpoint which encourages the conservative approach of keeping the data close to yourself (i.e. on-premise).

There's no denying however that the cloud is here to stay, and enterprises do have to strike a balancing act between the economic argument of moving to the cloud while weighing off the regulatory risks in doing so. In fact, we have spoken with some customers who are in the midst of their digital transformation journey and are excited about the move to the cloud. But several are under the mistaken impression that when they outsource their IT infrastructure to the cloud provider, they're also outsourcing their accountability. And nothing can be farther than the truth!

Regulations always hold the data controller – the one who primarily collects data responsible for data breaches or losses.

Don't be fooled, not even for a second. Regulations always hold the data controller – the one who primarily collects data responsible for data breaches or losses. The data processors (the cloud providers), usually don't have to live up to the same standards of accountability.

GDPR for the first time, places some level of accountability on data processors as well, although data controllers bear the brunt of the responsibility without a doubt.

Data is also shifting from traditional data centers into the hands of end-users, or more precisely, endpoint devices – like laptops, tablets, and mobile phones. Users are getting used to a world where they access data at their fingertips, and the cloud is just a hotspot away. Regulations thus make it critical for businesses to also protect the data on their user endpoints – an oft-neglected area.

If you're a company that does business or collects data of anyone residing in the EU region, GDPR is non-negotiable. What you could do though, is to be aware of how to understand and implement GDPR for your business.