Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

General Data Protection Regulation, (GDPR):

What, Why, How and What Next?

Introduction:

On May 25, 2018, across Europe, the general data protection regulations or GDPR started to be enforced. GDPR has modernised the laws that protect the personal information of individuals within the European union (EU) and beyond. As we live in data-heavy lifestyles and people (more so young children and teenagers) routinely sharing their personal information freely online; the need for GDPR was imminent.

GDPR was designed to "harmonise" data privacy laws across all European Union (EU) member countries as well as providing greater protection and rights to individuals. GDPR was created to lay out regulations as to how businesses and other organisations handle personal and non-personal data of any individual that interacts with them. The implication of potential large fines and reputational damage have made the effectiveness of GDPR come to life. For businesses complying with GDPR rules there is much trust and reliance among its userbase.

GDPR: In a Nutshell

GDPR is currently the world's strongest set of data protection rules, which enhance how people can access information about them and places limits on what organisations can do with personal data. The full text of GDPR is very comprehensive and contains 99 individual articles.

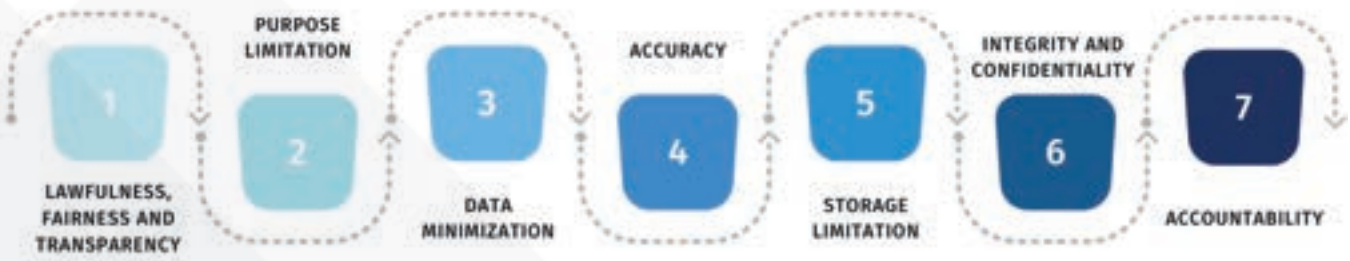
GDPR came into force on May 25, 2018. Countries within Europe were given the ability to make their own small changes to suit their own needs. The strength of GDPR as a strong data protection instrument has been a progressive approach to securing people's personal data and how data in general should be handled.

At the heart of GDPR is personal data. Personal data is that information that allows a living person to be directly, or indirectly, identified, for example: a person's name, location data, or a clear online username, or it something less apparent such as one's IP addresses and cookie identifiers can be considered as personal data. Under GDPR personal data also includes information about racial, ethnicity, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, health information and data around a person's sex life or orientation.

In a nutshell personal data allows a person to be identified, thus pseudonymised data can still fall under the definition of personal data. Personal data is important under GDPR because individuals, organisations, and companies that are either 'controllers' or 'processors' of it are covered by the law.

The GDPR's key principles

GDPR lays out seven key principles in Article 5. These principles are designed to guide how people's data can be handled. These principles act as an overarching framework designed to layout the broad purposes of GDPR. GDPR's seven principles are: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.



Data Minimisation:

The data minimisation principle is important as in the new age of broadband internet and an ever-increasing access of internet to rural and semi-urban places, there is such a high-volume of information creation. The requirement is that organisations do not collect more personal information than needed from users. Thus, data minimisation is identification of minimum amount of personal data needed to fulfil a purpose.

The principle is designed to ensure organisations don't overreach with the type of data they collect about people. For instance, it's very unlikely that an online retailer would need to collect people's political opinions when they sign-up to the retailer's email mailing list to be notified when sales are taking place.

Integrity and confidentiality:

Personal data is required to be protected against unauthorised or unlawful processing, as well as accidental loss, destruction, or damage. The GDPR requires appropriate information security protections to be in place and protection of information in general to make sure information isn't accessed by hackers or accidentally leaked as part of a data breach.

GDPR doesn't say what good security practices are, as they are different for every organisation. For example – a bank will protect financial information in a more robust way than one's local grocery store. GDPR highlights proper access controls required to be put in place. There is a direct corelation to the good cybersecurity measures to be in place mapped to the size and use of one's network and information systems.

Accountability:

Accountability is the only new principle under GDPR – it was added to ensure companies can prove they are working to comply with the other principles that form the regulation. Accountability principle means documenting how personal data is handled and the steps taken to ensure only people who need to have access to information are able to. Accountability does include training staff in data protection measures and regularly evaluating and data handling processes.

The "destruction, loss, alteration, unauthorised disclosure of, or access to" people's data must be reported to a country's data protection regulator where it could have a detrimental impact on those who it is about. This can include - financial loss, confidentiality breaches, damage to reputation and more. For companies that have more than 250 employees, there's a need to have documentation of why people's information is being collected and processed, descriptions of the information that's held, and how long it's being kept for and descriptions of technical security measures in place. GDPR's Article 30 lays out that most organisations need to keep records of their data processing, how data is shared and data storage.

The accountability principle is crucial for organisations to investigate when a potential cyber breach happens. An accurate record of all systems, information processing and the steps taken to mitigate errors is a good indicator to regulators that one's organisation takes its GDPR obligations seriously.

GDPR success story: 4.3 million citizens and businesses consulted the European Commission's online portal on the GDPR over the last two years . These December 2020 figures show that a large proportion of the EU population have heard about the GDPR and there has been a push by respective national data protection authority to make their businesses compliant to data protection breaches. There has been much effort in communication tools at the EU and the national level and towards making national procedures in compliance with GDPR guidelines.

GDPR Next phase:

The GDPR is still in its early stage and many countries will continue to monitor its progress as they consider how to craft and effectively enforce their own data protection laws. Democracies around the world such as Australia, Japan, South Korea, Brazil, and India have already modelled some part of their non-personal and personal data privacy legislation on the GDPR, which already talks about the success of GDPR in global context. Three years is a relatively short time but the success of GDPR shall lie in its enforcement enablement and faster resolution and penalisation of wrong doers.

The next phase of the GDPR's implementation within EU must address the following challenges:

- Creating new communication and collaborative tool for the national data protection authorities.
- Creation of additional guidelines to act as clarification and one-stop-shop solution to queries.
- Clarifying and increasing use of the urgency procedure; and
- Increasing the EU and national resources for data protection authorities.