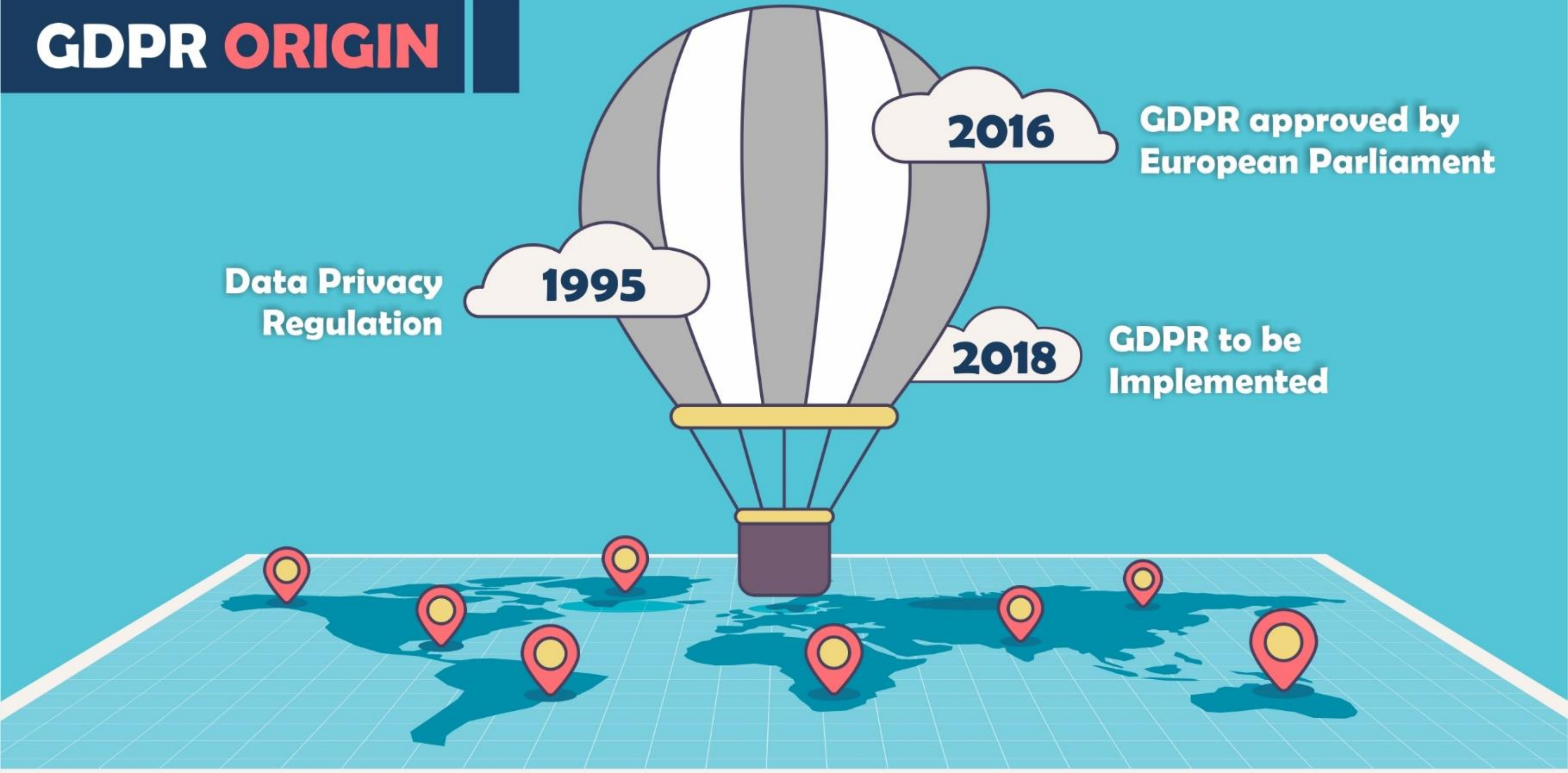
GDPR ORIGIN



OBJECTIVES OF GDPR

- Harmonize data privacy laws across Europe,
- Protect and empower all EU citizens data privacy
- Reshape the way organizations across the region approach data privacy

KEY CHANGES PROPOSED

- Higher priority to data protection for EU nationals
- Protection against unlawful use of data
- Organisations can be sued in case of breaches
- Breach leads to penalty of 4% turnover or Euro 20 mn

PRINCIPLES OF GDPR

- **Breach Notification** – Data breach “resulting in risk for the rights and freedoms of individuals”, must be notified within 72 hours. Customers and data controllers to be notified “without undue delay”.
- **Right to Access** – Individuals can access from data controllers information about weather or not personal data is being processes, where and for what purpose.
- **Right to be Forgotten** – In case the individual withdraws consent or the data is not relevant for the purpose it was collected, data must be erased.
- **Data Portability** - The right for a data individual to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.
- **Privacy by Design** - At it’s core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.
- **Data Protection Officers** - There will be internal record keeping requirement. DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

GDPR - General Data Protection Regulation

Date: 13th April 18

GDPR is being called the most important change in data privacy regulation in the last 20 years. With the implementation deadline of 25th of May 2018, organisations across Europe are gearing up to embrace the changes associated with the new regulation. This means scrutinizing processes, adapting technological changes and retraining resources responsible for managing, processing and maintaining consumer related data.

In this article, we aim to address GDPR holistically, making it useful for end consumers, organisations as well as overseas data processing centers.

We address the following areas:

1. What is GDPR?
2. What is the difference between GDPR and Existing Data Protection Act?
3. What are the benefits and risks associated with GDPR?
4. Who will be impacted by this change?
5. What can organisations do to be GDPR ready and compliant?

What is GDPR?

GDPR is a new data protection regulation that replaces the Data Protection Directive (94/46/EC) of 1995 and goes into effect on the 25th of May 2018. After 4 years of discussions and debates, GDPR was approved by the EU Parliament in April 2016.

GDPR focuses on the Human Rights of EU citizens, data privacy and rights of individuals based on the belief that consumers must be aware of what data is held about them, how is it maintained, used and discarded.

What is the difference between GDPR and Existing Data Protection Directive?

GDPR has six principles* compared to eight in the Data Protection Directive, with key focus on intent with which data is collected and used while being lawful, fair and transparent and used only for the purpose for which it was collected. GDPR also focuses on data being adequate, relevant and limited to what's necessary given the purpose of data collection. Additional focus is given on ensuring that data is kept up to date and also maintained in a form from which the subject can be identified no longer than necessary.

GDPR also aims at addressing technical and organizational measures being in place in organisations to protect against unlawful and unauthorised processing, as well as accidental loss or destruction.

GDPR also assigns accountability to organisations, in case of breaches or non-compliance fines can reach as high as 4% of the businesses turnover or €20m! This is making organisations take notice and act accordingly.

Overall, GDPR is assigning higher priority to data protection much as health and safety has been in the last few decades.

What are the benefits and risks associated with GDPR?

While GDPR helps safeguard end consumer's data and lowers the risk of data fraud in severe case and unauthorised and unsolicited data sharing in most cases. It also assigns accountability to organisations with severe financial penalties in case of breaches besides severe reputational loss.

GDPR impacts both the data processor and data controller and in most cases organisations (who process more than 5000 customer's data or has more than 250 employees) will need to appoint data protection officers with expert knowledge and a fair level of independence. In these scenarios, we may see a real shortage in expert consultants who can systemically guide organisations to a Data Quality Assurance framework. Organisations would also have to rely on expert process consultants to redesign processes, ensuring data protection is built within the processes.

Who will be impacted by this change?

All organisations that collect and process end consumers data will be impacted along with and third party processing center outside of EU that processes data belonging to EU citizens.

While UK is heading for Brexit in two years, GDPR gets implemented on the 25th of May. Organisations in UK would also have to comply with GDPR keeping in mind the financial and reputationsl loss in case of non-compliance.

What can organisations do to be GDPR ready and compliant?

Organisations need to address this important change systemically. Data protection and security would be given higher priority in organisations than it has in the last two decade.

Key challenges for an organisations can be summarized in three areas.

1. **Data Management (Process)**
2. **Privacy by Design (Technology) and**
3. **Data Processing (People & Practice)**

Data Management –

Data Management would encompass, data acquisition or collection, data sharing within and outside organization both within and outside of EU, data maintenance and data deletion. Organisations would need consultants with expert knowledge in creating governances, policies and framework for data management. Fit for purpose data needs to be defined, policies for sharing, maintaining and deletion must be clearly documented, adhered and governed to ensure GDPR compliance.

Privacy by Design -

Privacy by Design would encompass data protection from the onset of designing systems rather than an addition. Organisations may have to invest in technologies that allow data protection including Data Masking, encryptions, synthesis etc. Based on organisational needs processes and systems may have to be designed to build data protection into the system. Organisations may also have to invest more in proactive risk identification and mitigations, periodic tests and audits etc. External business and technology consultants would have to collaborate with organisational senior management in designing and deploying privacy designs.

Data Processing –

Data processing forms the core of the organisational ecosystem. Today the complexities of data processing is multiplied with involvement of multiple geographies and other business necessities. Organisations must ensure processes are compliant to GDPR, i.e. only data that needs to be shared is shared with the processor, data is used only for the purpose for which it was collected, data is maintained and kept up to date and most importantly data may not reveal the identity of the consumer. To ensure these organisations may have to re-think their processes and data processing strategy. While technology can play a role in ensuring data is masked or encrypted or broken to ensure the privacy of the consumer, processes also may need to be relooked to ensure that they are fit for purpose.

Closing Notes:

While it took 20 years for an important data protection regulation to be implemented in the EU, it would go a long way in protecting consumers in the EU.

Organisations would be held accountable for data protection and in turn would have to assign much higher priority to data protection given the penalty could be as high as 4% of turnover or €20m!

Organisations will have to maintain internal record keeping and have to hire Data Protection Officers.

Organisations may have to invest on Consultants expert knowledge for creating frameworks for Data Management, Data Protection by Design and Data Processing.

Companies in UK will have to be ready for GDPR given that Brexit is still two years away.

Sources

https://www.eugdpr.org/key-changes.html

http://cjel.law.columbia.edu/preliminary-reference/2017/mind-the-gap-loopholes-in-the-eu-data-privacy-regime/

https://gdpr.report/news/2017/05/17/gdpr-vs-data-protection-act-spot-difference/

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation