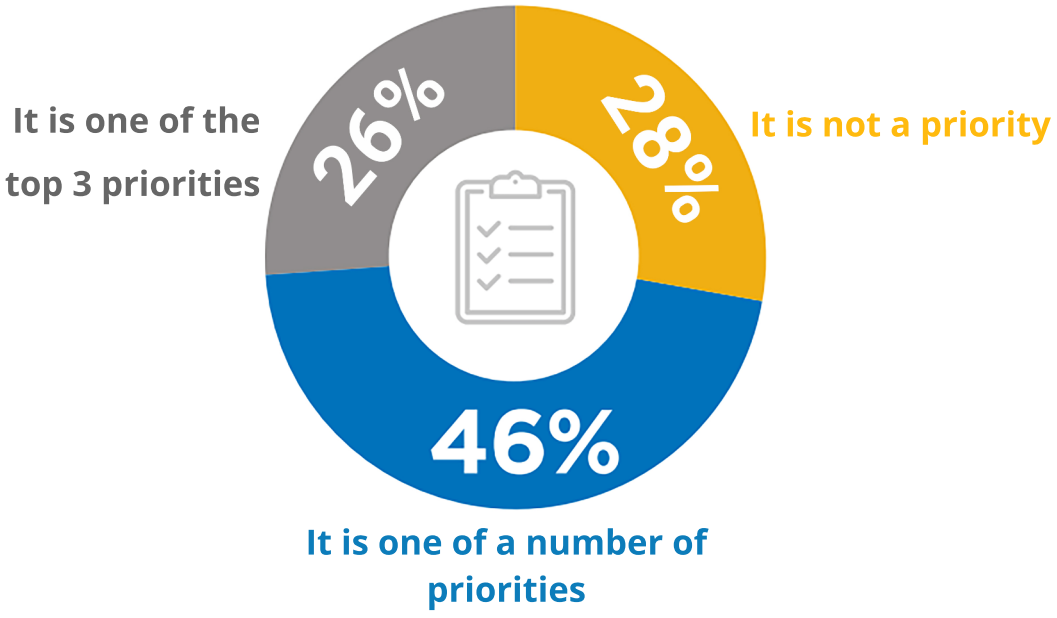
GDPR

SIMPLIFIED

CYRAATEK

The European General Data Protection Regulation (GDPR) will be enforced from 25th of May 2018. This regulation affects organizations that process personal data of European residents. Hence, this act affects majority of the businesses in the technology sector, as well as those who operate non-technical businesses, i.e. Hairdressers who maintain digital records of their clients.

This guide aims to make it easier for business to understand and implement changes required to comply with GDPR.



"With many companies being familiar with EU GDPR regulations, the next question was whether this understanding translated into a priority to be in compliance. A large proportion of companies indicated that compliance is a priority. " - **2017 EU GDPR Report**

Embracing GDPR

GDPR is the biggest legal change of the digital age.
- Mark Lomas

GDPR essentially allows EU citizens to gain more control over their personal data. Unlike the Data Protection Directive 95/46/EC, GDPR is being adapted by enterprises who understand the consequences of not being compliant. However, many SMEs are lagging behind.

In a recent survey conducted by Veritas Technologies, it was discovered that 86% of the organizations understand and acknowledge that they will suffer negative consequences if they are not compliant with GDPR. However, they lack knowledge, resources and finances to implement changes needed to be compliant with GDPR.

The good news is that in spite of the major changes in the way data will be handled from May 2018, foundation of GDPR has been derived from existing data protection regulations. So, as long as the businesses are compliant with existing laws, they should be able to achieve GDPR compliance with minimal effort. Additionally, embracing GDPR will also help companies improve their reputation, and consequently gain more business.

It must be noted here that GDPR also applies to organizations that handle data of European residents but are based outside of the European Union. Hence, a fair amount of businesses comes under the scope of GDPR.

GDPR Challenges

1. Multiple new requirements

European legislators are on a firm intent to increase accountability for businesses which handle personal data. Therefore, with this introduction of GDPR, Businesses and Enterprises are being encouraged to demonstrate that they have taken steps to ensure that data is safe. Furthermore, to encourage transparency, obligations, rules and procedures listed in the GDPR will also need to be implemented by the businesses. For instance, rules about the right to be forgotten and data portability will have some impact on companies, as they will need to amend their procedures and machines to accommodate such rights and requests.

2. Process-driven directive

GDPR has set out specific processes for the companies to adapt. The idea presented by the directive is to help companies structure and formalize certain areas like data protection and digital communication. By enforcing these specific procedures in place for businesses to adapt, general consensus is that companies will work more efficiently and at the same time achieve compliance with privacy rules.

For example, data protection impact assessment or PIA will become mandatory under GDPR directive. Hence, companies will need to complete this assessment before engaging in any data processing which may involve risk to the rights of consumers. Additionally client privacy principles will need to be incorporated in every process and procedure by default. Additionally, companies are also highly encouraged by GDPR directive to certify their data processing with a reputable third party or Government owned approved certification body for maximum compliance.

Biggest change to EU data protection law for two decades.
- SC Magazine

GDPR also imposes concrete measure which businesses have to implement in relation to their activity regarding data protection. Furthermore, the directive also enforce the companies to disclose any data breach to authorities without undue delay, as well as a documented report of underlying facts, effects and remedial action taken to secure the systems and data from further breach.

GDPR also encourages companies to create new roles, i.e. a position of Data Protection Officer (DPO). This position becomes mandatory for businesses engaging in profiling or tracking online behavior or for companies processing public health data.

3. Heavy penalties

Companies failing to comply with GDPR can face huge repercussions. By the directive, authorities will have the permission to take one or more of the measures listed in the GDPR

(i) Issue a warning or impose a temporary or definitive ban on processing personal data, OR

(ii) Impose a fine up to EUR 20,000,000 or 4% of the total worldwide turnover, depending on the circumstances of each individual case, OR both.

4. Implementation can be a challenge

As more guidance on GDPR is still forthcoming, it remains difficult for some companies to implement all of the requirements listed in the directive. Yet, at the same time a proactive approach is needed to avoid leaving it too late and risking a fine. For example terms used in the directive such as “undue delay” and “disproportionate effort” will need to be further clarified by the legislators, courts and regulators.

5. Support from the top management

Due to the implications listed above, board level support and resources are needed to implement changes required by GDPR across the company. Measures for instance fact finding, objective gap analysis, realistic milestones and clearly defined roles will help businesses introduce and establish changes needed to be compliant with GDPR .

The Road to GDPR Compliance

Once GDPR regulations comes into effect, this new law will strengthen data protection for EU citizens and changes how businesses approach information security, data privacy and overall IT governance within an enterprise. The legislation is pivotal for businesses operating in Europe because GDPR sees the introduction of mandatory security notifications. Under the GDPR, data breaches are fined up to four percent of global turnover of a business.

GDPR compliance is complex but it can be achieved through some simple steps:

- First develop company-wide awareness of the legislation and help colleagues understand how it affects the business.

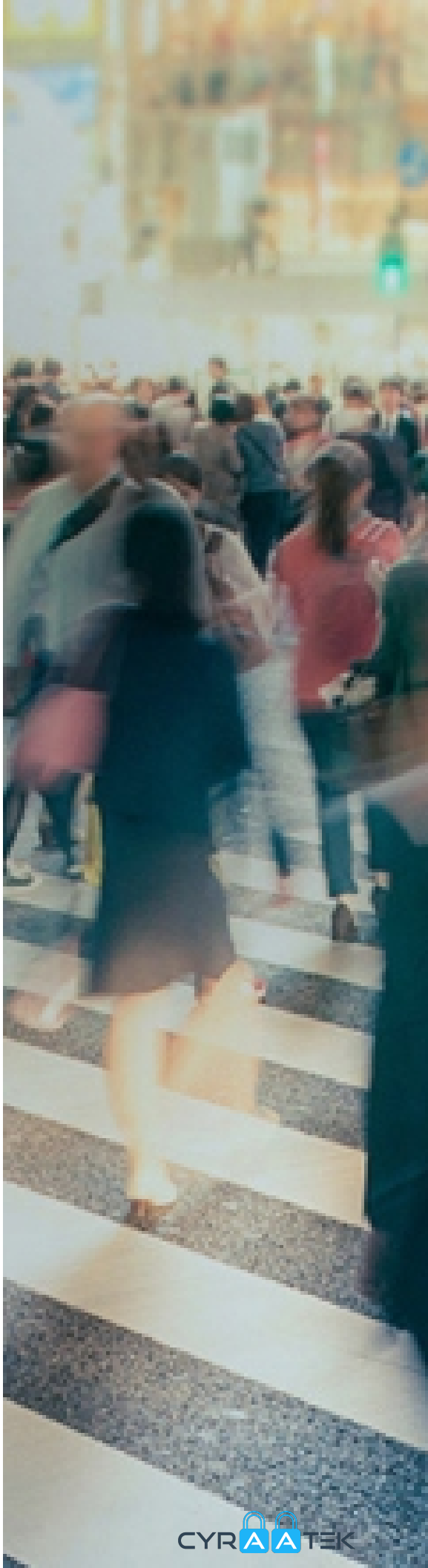
- Help the board understand the legislation and the resources required to transform how the organization handles personal data.

- Appointed chief data officer should drive GDPR compliance internally and if required a data protection officer should assess the data protection requirements

- Audit and review existing systems, procedures and contracts with suppliers and conduct an information audit.

- Businesses should also assess privacy notices and procedures.

- Ensure that the right procedures are in place to detect report, investigate and mitigate security breaches. GDPR requires companies to report any breaches within 72 hours of first detection.

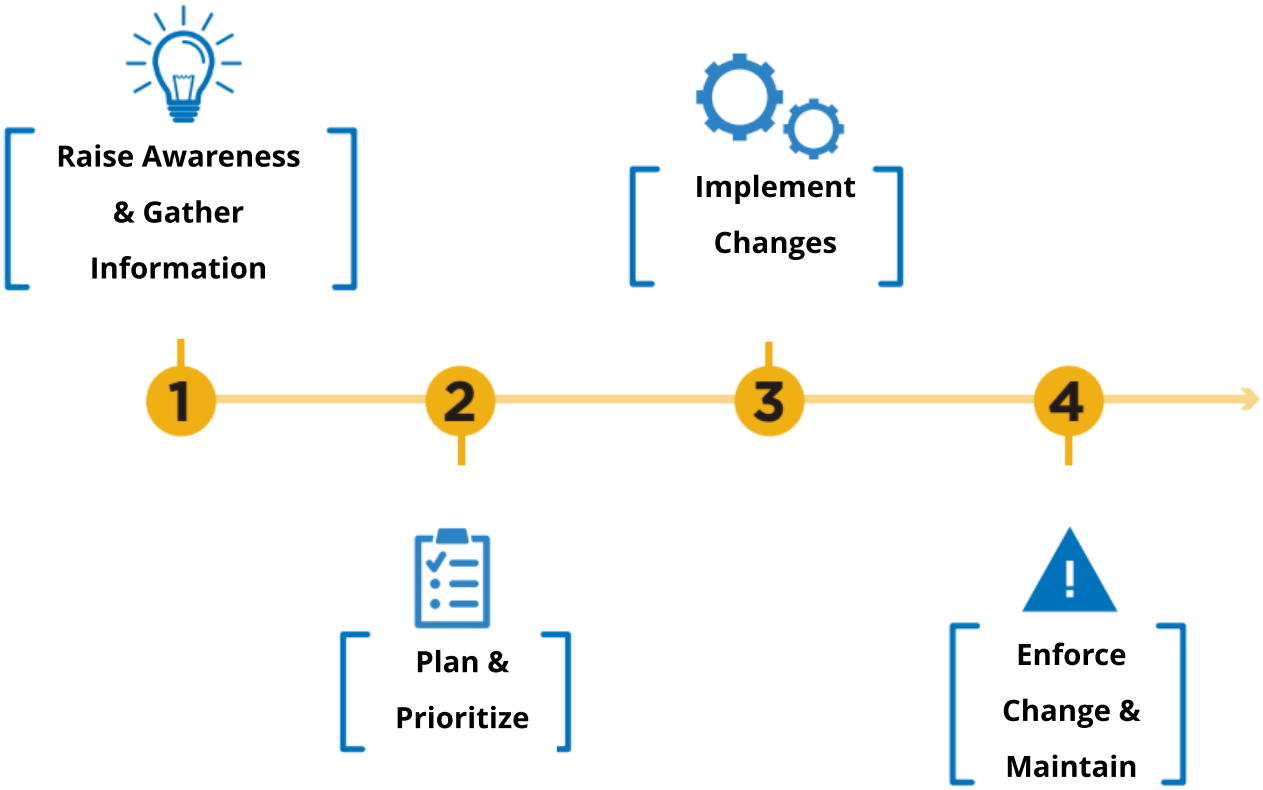


Conclusion

To become compliant with the directive, organization wide changes are needed by many businesses to ensure that personal data is processed in compliance with GDPR requirement. In many organizations, these changes means re-designing systems and procedures which deal with personal data, acquiring new systems and softwares and re-negotiating contracts with third party processors to ensure that they as careful and compliant with the data handling laws as you are.

Businesses therefore should start investing their time and effort in planning and implementation of changes as failure to do so could mean that businesses are left with new requirements to implement, without sufficient time or resources to do so.

For further advice and assistance on implementing changes relating to GDPR, contact our team of professionals at **enquiry@cyraatek.com**.



GDPR Preparation Timeline