Your FREE Guide from Tessolve Semiconductors Private Limited

Data Security Guide to GDPR

On the 25th May 2018 the EU's General Data Protection Regulation (GDPR) will come into place, which is the most stringent and burdensome privacy mandate in the world. Will you be prepared?

Data Security Guide to GDPR

Are you ready for the 25th May 2018?

Do you know what GDPR stands for? Are you ready? In less than 1 years' time on the 25th May 2018 the EU's **General Data Protection Regulation (GDPR)** will come into place, which is the most stringent and burdensome privacy mandate in the world. Don't think that it won't happen due to Brexit. It will happen and doing nothing is likely to leave you with the huge fine!

The following Tessolve security guide will highlight the main aspects of GDPR and the key areas to consider regarding data security.

GDPR Overview and Impacts

Companies that operate within the EU now need to take extra precautions to ensure the safety of their data or face a fine of up to 4% of global turnover. GDPR applies to any organization that owns, holds or processes European data or is based in the EU. Companies need to start preparing now to navigate through the complexity involved in addressing GDPR to comply fully with the regulation.

The existing data privacy laws date back to 1995 with the data protection Directive 95/46/EC' in the EU and the UK 1998 'data protection act'. Both were comprehensive for their time but have since become outdated due to the explosion of data and the use of technology across the EU as companies share more consumer information. The GDPR is aimed to address these factors enabling EU citizens far greater control over their personal data.

GDPR is the biggest change in European data laws in the last 20 years. It is being implemented to ensure companies raise the bar on data protection to rebuild consumer trust. It will force companies to take a proactive view of their data policies and strategies. There must be accountability, responsibility, and the ability to demonstrate data privacy plans and implementations. The Information Commission Office (ICO) will be enforcing and breaches will be severely punished.

Everyday there are new headlines of consumer data being misused or security concerns with data being hacked. The largest most recent high-profile event was the data stolen from TalkTalk in 2016 by a 17-year-old boy who then tried to blackmail the organisation. 160,000 customer records were accessed. The estimates are this event has cost TalkTalk directly / indirectly in the region of £60million, plus what about the ongoing brand damage. The list of other companies also targeted and brands effected include household names such as: Asda / Three Mobile / Tesco bank / Morrison's / Moon pig / Sage / Wonga.

TalkTalk has been fined a record £400,000 fine for security failings which led to the theft of personal data of almost 157,000

The cyber attack in October last year exposed the latest security failure for the company, which was forced to admit it had not encrypted some personal details of customers.

The Information Commissioner's Office (ICO) said the attack could have been prevented if TalkTalk had taken basic steps to protect customers' information.

INDEPENDENT

GDPR comes at a time when consumer trust needs rebuilding in how organisations use and protect our personal data.

Data Security in GDPR

Below gives an overview of the key articles (25, 32, 33, 34 & 35) in the GDPR that relate to data security:

The following are excerpts of the full articles. For the full regulation please see: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Article 25

Data Protection by Design and by Default.

The controller shall determine means for processing and implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 32

Security of Processing

The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- The Pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Article 33

Notification of a Personal Data Breach to the Supervisory Authority.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Article 34

Communication of a personal data breach to the data subject.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication to the data subject referred shall describe in clear and plain language the nature of the personal data breach.

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met if the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption

Article 35

Data protection impact assessment.

Where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The assessment shall contain at least the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Summary

GDPR is going to drive the standard for data protection across Europe and the rest of the world. Companies must comply with the regulation or there is a high chance they will be subject to a large fine. Organisations must ensure the data they hold is safe and be able to demonstrate the following data security best practice:

- Security by Design – Don't wait to come under attack, build in application security from the start.
- Regular Security Testing - Discover vulnerabilities, assess their likely impact, recommend fixes and ultimately help protect your business.
- Security gap analysis – To review security approach is up to date and continually evolving with the threat.
- Ability to Restore Data – Perform regular testing of backup and restore of data.

Tessolve Recommendation

Companies should look on GDPR as a positive and utilise compliance as a way to demonstrate security best practice to ensure customers continue to trust in their brand.

asureSECURE

Let Tessolve help ensure you are ready for the 25th May 2018, guiding you through the challenging data privacy environment and compliance to the latest international regulations. Our team of data privacy experts will review where you have GDPR data stored and present recommendations on improvements. In parallel, our 360- security team will analyze your infrastructure for potential weaknesses, provide security by design best practice and assistance in ongoing security measures.

Discover how Tessolve can help with your Data Security & GDPR

www.tessolve.com