magentrix

Security Policies and GDPR Guidelines

What is the GDPR?

The GDPR is a European Union regulation that establishes a new framework for handling and protecting the personal data of EU-based residents. It came into effect on May 25, 2018.

Personal data plays a big role in our day to day business operations. It is critical that people have control and clarity over how their data is used and protected organization, and that organizations provide clear guidelines to protect their personal data.

One of the goals of GDPR is to bring data privacy laws across Europe up to speed with the rapid technological change in the past decades. It builds upon the current legal framework in the European Union, including the EU Data Protection Directive in existence since 1995.

Who does the GDPR affect?

The GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What constitutes personal Data?

Any information related to a natural person or "Data Subject", that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Magentrix's GDPR Commitment

We are committed to our customers' success, including compliance with the GDPR.
In addition to existing privacy laws, compliance with the GDPR requires a partnership between Magentrix and our customers in their use of our services. Magentrix will comply with the GDPR in the delivery of our service to our customers. We are also dedicated to helping our customers comply with the GDPR.

How will Magentrix comply with the GDPR?

- Trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your information seriously.
- Magentrix places the utmost importance on data protection and has a track record of staying ahead of the compliance curve.
- Magentrix's Legal, Trust and Privacy teams have carefully analyzed the GDPR and are undertaking the necessary steps to ensure that we comply.
- Magentrix has set up the following responsibility guide to ensure compliance:
    - **Build in design and architecture to protect your data:**
      Magentrix has been designed from the ground up with security in mind. Records can be secured based on access levels, security groups and sharing rules.

- **Secure networks:**
  Magentrix has put in place necessary Security Appliances and Monitoring tools and firewall rules in order to make its network secure. Magentrix performs regular Penetration testing to make sure its network is secure.

- **Data encryption:**
  Magentrix secures the “Data in transit” and “Data at rest”. To protect the data in transit, Magentrix uses SSL (Secure Socket Layer) and TLS (Transport Layer Security) for data transfer, creating a secure tunnel protected by 128-bit AES Encryption. For “Data at rest” Magentrix uses 256-bit AES Encryption to secure the data.

- **Limited employee access:**
  We know that as a customer you expect us to be responsible with your data. As part of this responsibility, we make sure that only key Magentrix employees have access to our production networks.

- **Employee awareness:**
  As part of keeping our services secure, we also make sure that our employees are trained and are aware of security and privacy issues. Therefore, we make sure that our employees understand and acknowledge security policies prior to being granted system access.

- **Right to be forgotten:**
  Any request with regards to the “Right to be forgotten” must be sent to support@magentrix.com. Our support team will work with you to make sure of the proper removal of the requested data.

- **Breach notification:**
  Magentrix is committed to notify the data protection authority within 72 hours of noticing a material personal data breach, provide the nature of the breach and provide an estimate of how many people are likely being impacted. Furthermore, Magentrix is committed to taking the appropriate measures necessary to mitigate the breach.

- **Data minimization principle:**
  Magentrix keeps as little data as necessary. At the same time Magentrix provides the necessary tools to the data controller to restrict and make sure only data necessary is available.

What are your obligations under the GDPR?

- It is important to remember that you, as the business customer and the data controller, have specific legal obligations under the GDPR.

- You should be confident that any providers (data processors) which you work with have a highly robust approach to data protection, understand the obligations of the GDPR and are well prepared to meet them.

Key changes to GDPR

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Privacy by design:

This means that organizations handling personal data need to think about data protection when designing systems, not just review privacy implications after a product or process is developed. If you process a lot of data or deal with sensitive information, in many cases you will also need to conduct data protection impact assessments to meet the privacy by design principle.

User rights

The GDPR expands the existing set of user rights and creates several entirely new rights. Companies should review and ensure they have effective systems in place to give effect to these rights.

Tougher breach notification rules

Organizations are required to have a strong breach notification system in place and understand their specific reporting obligations.

Accountability

Companies must now adhere to the principles set out in the GDPR, as well as demonstrate that compliance is in line with the principle of accountability. This requires a comprehensive and clear internal privacy governance structure.

Data protection officer

The GDPR requires companies that engage in processing of EU user data to determine if they should appoint a Data Protection Officer. Companies that routinely process large volumes of information or particularly sensitive information should consider appointing a DPO.

Disclosing Personal Data

Your personal data will not be shared with other parties, except where your explicit consent is given to us. Under certain circumstances, the data protection act allows your personal data to be disclosed to law enforcement agencies without your consent. Under these circumstances, Magentrix AS will disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisors where necessary.

Data Retention

Customers choose how long to retain Customer Data, including Personal Data, on the Magentrix Platform. Unless otherwise specified in the contract, Magentrix does not delete Customer Data, including Personal Data, during a subscription term, unless the customer instructs Magentrix to do so. After a customer's contract with Magentrix terminates, Magentrix deletes Customer Data within 30 days.

Security Controls

Magentrix platform include a variety of configurable security controls that allow customers to tailor the security of the Services for their own use.

Security Policies and Procedures

Services that Magentrix provides are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID and source IP address (when available).

- If there is suspicion of inappropriate access, Magentrix can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Magentrix personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

Security Logs

All systems used in the provision of the Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server in order to enable security reviews and analysis.

Physical Security

Production data centers used to provide the Magentrix Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.