MATRIX42

EGOSECURE DATA PROTECTION

In line with the GDPR

Achieve full compliance in 7 minutes

Challenge:
Fulfilling the requirements of GDPR

The General Data Protection Regulation (GDPR) entered into force on 25 May 2018. It harmonises data protection law within the EU. The GDPR applies to all companies domiciled in the EU and certain non-European companies. Personal data are to be protected. In the event of a violation, in addition to a possible loss of image, a maximum fine of either 20 million euros or up to 4% of the total worldwide annual turnover of the old financial year is imminent.

The fine should be as deterrent as possible, which is why the higher of the two amounts is chosen.

All companies must ensure that their security architectures comply with the applicable guidelines. With Matrix42 EgoSecure Data Protection you can do it in 7 minutes.

This is how EgoSecure Data Protection supports you

EgoSecure Data Protection offers a complete solution portfolio with which you can immediately implement the legal requirements of Articles 25, 32, 33 and 34 (GDPR).

Privileged user access control (Article 25 + Article 32 GDPR)
EgoSecure Access Control and Application Control ensure that no one has unauthorized access to applications, devices or specific file types.

Preventing attacks through data encryption (Article 32 GDPR)
Encryption is an important part of the security measures EgoSecure Data Protection is equipped with. By implementing encryption solutions, data storage devices are effectively protected. In addition, privileged user access control ensures that only authorized persons have access to applications, devices or specific file types.

Audit data, control and behavioral analysis (Article 30 + Article 33 GDPR)
The Audit and Insight Analysis modules monitor all data movements and access in real time. They automatically send notification of specific behaviors to a pre-defined location.

Notification of data protection violations (Article 34 GDPR)
EgoSecure Data Protection automatically monitors all data transfers through the audit function. Audit-proof logging of unencrypted file transfers ensures that data protection violations are detected and documented.

MATRIX42

Your Benefits

For companies

- Compliance with GDPR requirements (Articles 25,30,32,33,34)
- Easy integration into existing IT infrastructure and low hardware requirements
- Consideration of the minimum standards of the BSI
- Data access only by authorized persons
- Passing on and storage of data only in defined ways
- Reliable support with excellent SLA compliance
- Workers council and data protection compliant behaviour analysis and auditing

For IT departments

- Reduced complexity due to clear application and device control
- Transparent overview of all data movements and possible weak points
- Automation of behavior-based protective measures
- Easy installation and configuration of the software in a few hours
- Rapid implementation of data protection guidelines, e.g. data storage in the cloud
- No additional effort for the support team

For end users

- Users don‘t have to get used to it
- No user training required
- Automatic encryption and decryption of files on all devices and storage locations without the need for end-user intervention

3 Reasons to choose Matrix42 EgoSecure Data Protection

1

Rapid implementation of GDPR regulations

As a German company, Matrix42 has always been guided by the requirements of the Federal Data Protection Act (BDSG). The complete range of functions consisting of access control, encryption, logging and automation helps the company to implement the GDPR in 7 minutes and to set up an individual protection concept without loss of productivity of the employees.

2

Safety that creates joy

Matrix42 EgoSecure Data Protection protects your business without changing the way you work. Users don‘t notice anything and IT doesn‘t need any extra training. This is well received by the users and relieves the support and IT teams. Everything runs as before, but on a higher security level.

3

Making IT security transparent

The Insight Analysis monitoring tool collects all data movements in the network for you and prepares them graphically. Secure Audit makes the data flows visible in detail, shows possible weaknesses in the protection settings and enables forensic information to be determined. IntellAct evaluates the facts collected by Insight Analysis and can automatically trigger appropriate protection measures.