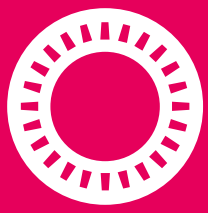


MATESO
PASSWORD SAFE

Whitepaper EU-GDPR Article 32

Introduction

The European General Data Protection Regulation now provides a uniform legal framework for what was previously a matter of interpretation. Since 25 May 2018, the EU GDPR has prescribed the handling of personal data for companies.

Digitization and the associated growth in data volumes, as well as globalization and the resulting economic interdependencies across national borders, have made it urgently necessary to standardize data protection.

This whitepaper deals with how Password Safe can be used in a data protection compliant manner and therefore refers to Article 32, „Security of processing“ in particular.

Using Password Safe compliant with GDPR, article 32

In order to ensure proper data processing, technical and organisational measures are absolutely necessary. These required EU-GDPR security guidelines in accordance with Article 32 can successfully be implemented with Password Safe.

The technologies and tools mentioned in the document refer to the current status as of 01.04.2021.

GDPR Article 32: Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

EU GDPR, article 32, paragraph 1, sentence 1:

»Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.«

The Solution with Password Safe:

To provide an adequate level of protection, the core technologies of Password Safe are constantly updated:

- Password Safe uses encryption technologies as well as hashing features (100.000 PBKDF2 iterations).
- The algorithm for data encryption used by Password Safe can be individually measured to the rising risk of attacks. With an increasing processing power, it is also possible to raise the key size for more security.
- The resilience of the systems regarding encryption, architecture as well as code analysis is constantly validated by external penetration tests.
- We do not run any outsourcing solution to provide internal security. Furthermore, our developers regularly participate in safety trainings.
- The quality label »IT Security made in Germany« by the TeleTrusT initiative proves the trustworthiness and reliability of the company and its software. MATESO is hereby obliged to fulfill the requirements of the German data protection law.
- The software is updated 3-4 times a year. In addition, the release of hotfix versions can react to and neutralize critical vulnerabilities as quick as possible.
- Our distribution partners are constantly trained to be up to date with new versions and updates of Password Safe.

The Solution with Password Safe:

1a.

» the pseudonymisation and encryption of personal data;«

- The data in Password Safe is reliably protected by end-to-end encryption (AES256, RSA4096, TLS1.3).
- Only one e-mail address is required to use Password Safe. Further personal data is not required.
- Due to the role-based assignment of rights, no direct connection can be made in the database between a user and the data or passwords stored by him.
- The data can only be decrypted by the creator or by persons authorized by him.

1b.

» the ability to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing in the long term;«

- Thanks to high availability, users can access their data from several Password Safe servers.
- With the security concept of our stateless multi-tier architecture, Password Safe is highly scaleable.
- The connection between systems can only be established through trusted certificates.
- Security mechanisms like audit-compliant logging provide reliable protection against manipulation.
- Password Safe uses Microsoft Communication Foundation as well as MS SQL for an efficient and fail-safe operation.

1c.

»the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;«

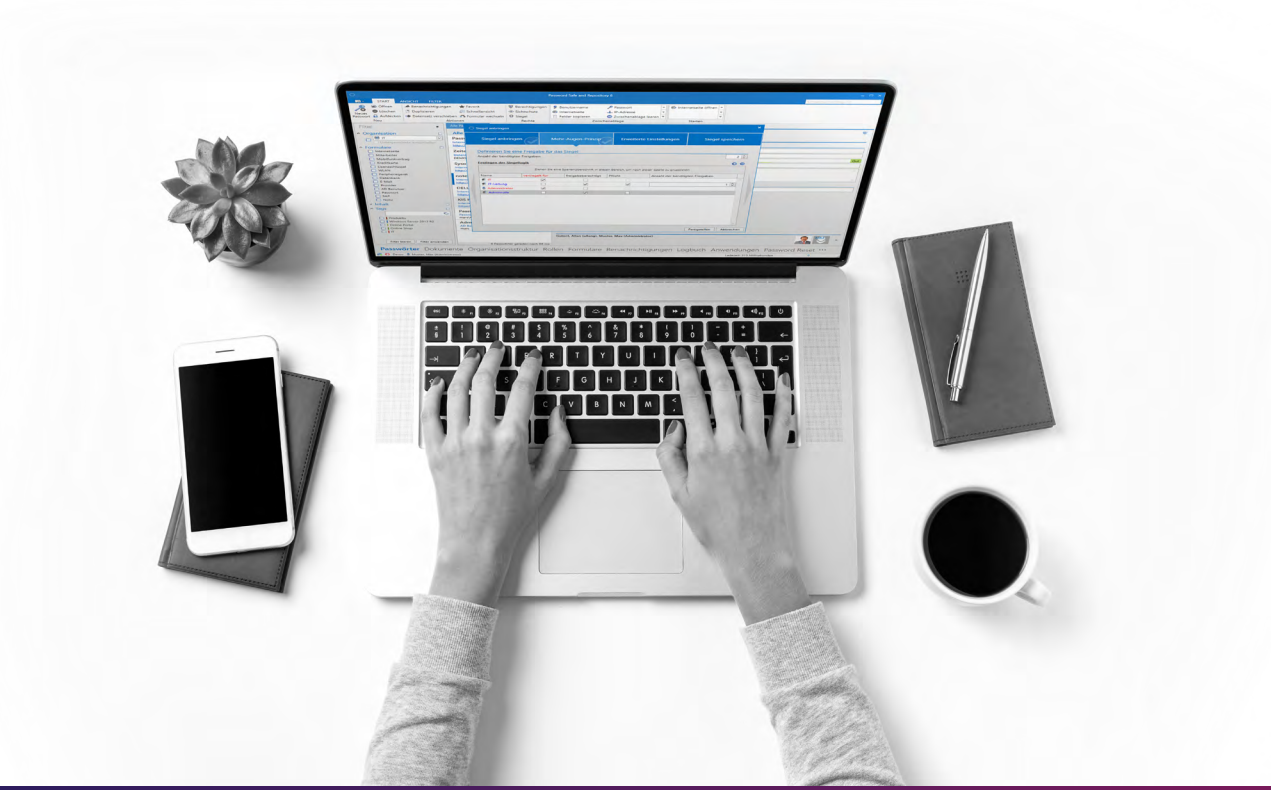
- The MS SQL backup system is used for backups and controlled by Password Safe.
- External MS SQL backup systems are compatible with Password Safe. This can minimize the risk of new, unknown backup systems.
- The emergency WebViewer offers an export file which is protected by two-factor authentication. If no backup has been created, the user can access the file system independently.
- The data of authorised users can also be held offline upon request.

Password Safe offers numerous options for backing up your data and restoring it in an emergency.

1d.

»a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;«

- If a certificate is not trustworthy, Password Safe automatically stops the communication and runs a security warning.
- Each data access is recorded GDPR-compliant in the logbook. The integrated filter function allows fast tracing of who had access to which data.
- Users profit from records that can be produced manually or periodically.
- The real time notification system ensures that users are always informed about important events in the data base so they can react directly.
- The predefinition and review of individually defined password regulations assures a safe processing of the Password Safe data.
- You can create restricted users for security audits. This ensures that right structures and company policies can be audited through external data access without having to uncover any passwords.
- The syslog server connectivity additionally guarantees tamper-proof data storing.



The Solution with Password Safe:

2.

»In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.«

- If it comes to loss or modification, the data inventory can easily be accessed or restored quickly with the rights-protected data history.
- The password masking effectively prevents data disclosure of unauthorized parties. Thereby, the user can still apply the hidden password for RDP and SSH connections as well as SSO on websites easily.
- Particularly security-critical data can be protected by multi-control principle. With the seal function, passwords have to be released by an additional user before they can be revealed.

3.

»Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.«

- To ensure flexible user control, Password Safe accurately depicts the granting of rights through its rights management.
- The user can set individual rights templates for passwords, documents or forms. Company guidelines are implemented true to scale – including special rules of conduct.
- The passwords can only be used on target systems via SSO agent or LightClient.
- To proof law-consistent implementation externally as well, the data can be exported and printed.

The fair and transparent processing of data in Password Safe is guaranteed by the rights system.

4.

»The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.«

- User rights can be granted or removed manually down to field level.
- Through the setting of temporary rights, subordinates are only granted temporal access to specific data.
- By using the seal feature, those responsible have to permit data access for users in the first place.

The processor can individually grant or remove privileges of any natural person under his authority.


MATESO

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE