Information Security

Pharius

Demonstrably compliant.

Cybercrime & security

Unfortunately, cybercrime is a reality, and so information security has taken on great importance. We would like to acquaint you with several important features of the array of precautionary measures that RDMG Publishers has taken for its Pharius application.

The array of measures with which we and our providers work includes the datacentre, hosting environment, backups, architecture and administration, OWASP (open web application security project), password security, vulnerability scanning, SSL security, safe design and administrator access. This array of measures and its internal consistency lead to a high level of security for the data of our valued customers and users.

Datacentre

Hosting and storage are housed in the modern Dutch datacentre BIT in Ede.

In addition to ISO certification, the datacentre is also NEN 7510 certified. This certificate applies to the areas of development, provision and support of (cloud) services, connectivity and managed IT services. The best practices of ISO 27002 are applied.

The datacentre is part of a network of three widely separated datacentres. This makes diversion to one of the other datacentres possible if necessary. In addition, they are interconnected by redundant fibre-optic connections.

The provider guarantees 99.9% uptime. The web-servers are monitored 24/7 for malfunctions, data traffic, disk capacity, load and (anomalous) use.
If an anomaly occurs it is detected immediately and action is taken.

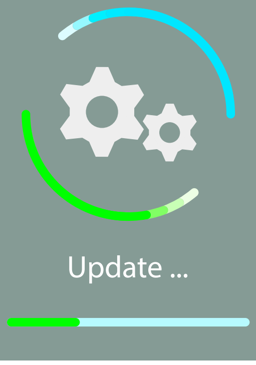
Access control for the datacentre is organised by means of a pass system in which logging is externally registered.

With regard to intrusion, the datacentre is BORG class 3 secured and equipped with an extensive intrusion prevention system with immediate notification of the control room. An electrified fence around the property and a CCTV system provide additional safety.

As for fire, all the data floors are equipped with an aspiration system. This system is capable of detecting fire in an extremely early stage. Gas extinction is activated via optical smoke detectors (mounted both above and below the data floor) if a fire is actually detected. The fire brigade uses the datacentre for drills and so is completely familiar with the building and the equipment present.

Hosting environment

Data storage is kept separate from the application by using multiple servers. The data storage is not accessible from outside, but only from the internal network. Our servers are equipped with the latest security updates and are actively maintained and monitored.

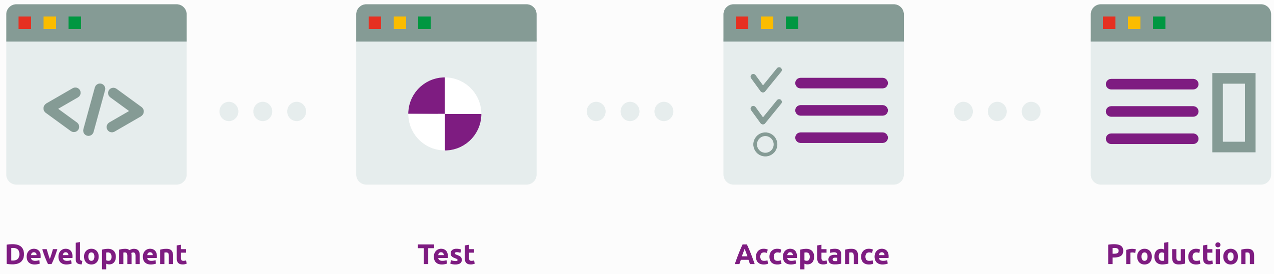


Backups

All data are secured daily using software solutions for automatically performing backups. The backup is made on a separate server in a separate, secure location and is not accessible from outside.

Architecture and administration

Pharius is based on a DTAP structure.
This means that there is a Development, Test (internal), Acceptance (external) and Production environment. The environments are strictly separated and there is a strict release policy.



Development

Test

Acceptance

Production

OWASP

The “Open Web Application Security Project” maintains a top 10 of greatest threats.
RDMG Publishers follows the recommendations and the top 10 of the OWASP closely to keep the security level optimal.

Password security

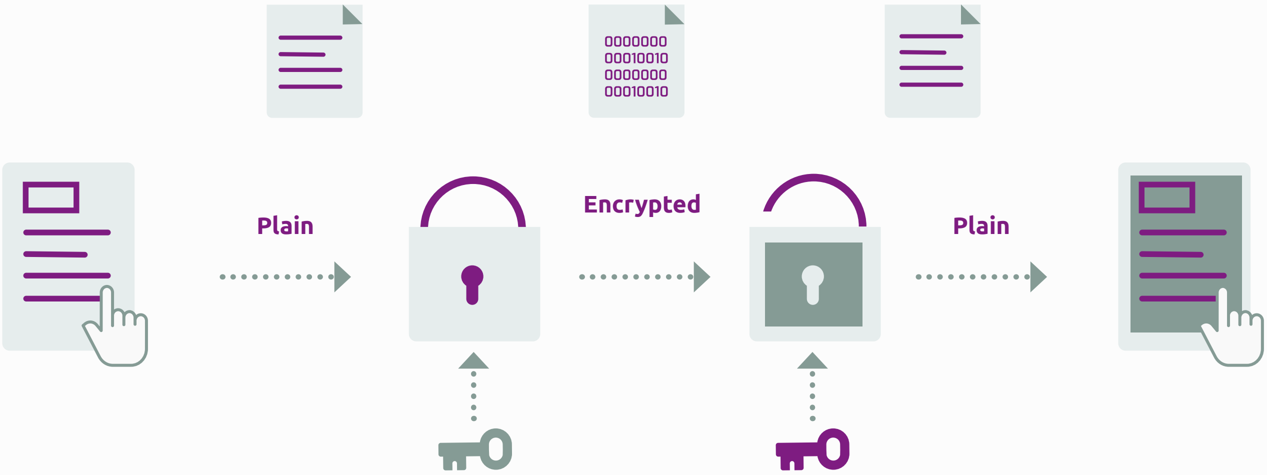
Pharius uses proven hashing algorithms to secure user passwords.

Vulnerability scanning

RDMG Publishers has high-end software to automatically scan and report on the security of Pharius.

SSL security

Data transfer between the browser of the end user and the webservers is secured with an SSL certificate.
This way, all the data sent and received are encrypted so that data cannot be intercepted by a malicious party.



Safe design

Every change or new functionality is subject to a change management policy to ensure that all changes in the application are authorised before they are put into production.

Our robust security framework based on OWASP standards, implemented at the application level, offers functions to limit threats such as SQL injection, cross-site scripting and DOS attacks at application level.

Provider guarantee

Our web development provider is an experienced developer of web-based software like Pharius. The company is ISO 9001 certified. RDMG Publishers has concluded a Service Level Agreement (SLA) and a Data Processing Agreement with them in the framework of the GDPR. The employees are contractually bound to confidentiality and have expertise in information security.

Personnel guarantee

Employees of RDMG Publishers are bound to strict confidentiality regarding customer data by means of their employment contract. If their employment ends, access to our application is blocked immediately.

Administrator access

We use technical access controls and internal policy (ISO certified) to prevent employees having arbitrary access to user data. We abide by the principles of rights with minimal privileges and role-based authorisations to minimise the risk of data exposure.

Access to production environments is maintained by a central system, verified by a combination of strong passwords, two-factor authentication and SSH keys. Moreover, we make such access possible via a separate network with strict rules and secure devices. We record all activities and monitor them regularly.

Pharius
Demonstrably compliant.