Technical and Organisational Measures / TOMs

Art. 32 GDPR / Security Measures

Stand: 2026-05-02

Security controls, access control, backups, monitoring and operational safeguards used by OpenDucks IT.

1. Purpose and Scope

These Technical and Organisational Measures describe the baseline safeguards used by OpenDucks IT to protect personal data, customer systems and operational environments.

The measures apply to services where OpenDucks IT acts as processor or operates infrastructure, support processes, hosting, managed services or software environments for customers.

2. Confidentiality

Access to systems is restricted to authorised personnel and service accounts. Administrative access is granted according to the need-to-know and least-privilege principles.

Accounts are protected with strong authentication where available. Shared administrative credentials are avoided where technically possible. Credentials are stored in protected password or secret-management systems.

Personnel and contractors with access to confidential information are bound by confidentiality obligations.

3. Access Control

User and administrator accounts are created, changed and removed according to operational need. Access reviews are performed when roles change, contracts end or a security event requires review.

Remote access is protected by encrypted connections. Administrative interfaces are restricted by role, network, authentication controls or equivalent protective measures where feasible.

4. Separation and Data Handling

Customer data is logically separated by account, system, tenant, service configuration or access boundary. Productive data is not used for testing unless required and legally permitted.

Data exports, support access and troubleshooting are limited to the scope necessary to provide the service or resolve the reported issue.

5. Integrity

Changes to managed systems are performed by authorised personnel. Relevant administrative actions may be logged in system, hosting, application or support logs.

Configuration changes, updates and migrations are planned with reasonable care and tested where proportionate to the risk and scope of the service.

6. Availability and Resilience

OpenDucks IT uses reasonable operational measures such as monitoring, backups, patching, capacity checks and incident response processes depending on the contracted service.

Backup scope, retention, restore responsibilities and recovery objectives depend on the applicable service description, offer or SLA.

7. Incident Response

Security incidents are assessed according to severity, affected systems, customer impact and legal notification requirements. Appropriate containment, mitigation and communication measures are taken.

Customers must report suspected compromise, abusive traffic, account misuse or data incidents without undue delay.

8. Regular Review

Measures are reviewed when services, risks, providers or legal requirements change. Technical and organisational measures may be adapted where this improves security or operational reliability without materially reducing the agreed protection level.

Kontakt

Fragen zu diesem Dokument können an legal@openducks.org gerichtet werden. Abuse-Meldungen bitte an abuse@openducks.org oder über die Abuse-Seite einreichen.