Security Whitepaper

Version 1

> ***Template — based on fotostudio.io's published security information. Pending legal review.***

Security Whitepaper

1. Introduction

This whitepaper describes how **Fotosoft SA** (operating the **fotostudio.io** platform) protects the data entrusted to it by professional photographers and studios. Security is built into our infrastructure, our software development and our day-to-day operations. We are the data **processor** for the personal data our customers upload; our customers remain the controllers (see the Data Processing Agreement).

2. Our approach

- **Security by design and by default** across the development lifecycle.
- **Data minimisation:** we process only the data needed to provide the service and never resell it or use it for our own commercial purposes.
- **Defence in depth:** multiple, independent layers of control rather than a single point of protection.

3. Hosting & infrastructure

- All data is hosted **exclusively in the European Union**.
- **Heroku (Salesforce, Inc.)** runs the application and databases; **Amazon Web Services (AWS S3)** stores uploaded files — both in European regions.
- The underlying data centres are certified to **ISO 27001** and **SOC 1/2/3**. These are certifications of our infrastructure providers, **not of Fotosoft**.
- Physical security (access control, environmental controls, 24/7 surveillance) is provided and audited by these data-centre operators.

4. Network security

- All traffic is served over **HTTPS/TLS 1.2+**; plaintext protocols are not used.
- Managed firewalls, network isolation and provider-level DDoS protection guard the perimeter.

5. Encryption

- **In transit:** TLS for every connection between clients, the application and storage.
- **At rest:** storage is encrypted (AES-256) at the infrastructure layer.
- **Credentials:** passwords are stored **hashed and salted** — never in clear text.

6. Access control & authentication

- **Least privilege:** staff access is limited to what each role requires.

- **Two-factor authentication** is enforced for administrative and server access.
- Customer data is **logically isolated per account**; uploaded files are served through secure, non-public links.
- Administrative actions are attributable to individual named accounts.

7. Application security

- A secure software-development lifecycle with **peer code review**.
- **Dependency and vulnerability scanning** as part of the build process.
- Protection against common web vulnerabilities (**OWASP Top 10**).
- Changes are version-controlled and traceable.

8. Availability & resilience

- Target service availability of **99.9% per year**.
- **24/7 automated monitoring** with alerting.
- **Daily backups** with geographic redundancy; restores are tested.
- Redundant, managed infrastructure reduces single points of failure.

9. Business continuity & disaster recovery

- Backups stored across multiple locations enable recovery from infrastructure failure or data loss.
- Documented recovery procedures aim to restore service with minimal data loss.

10. Vulnerability & patch management

- Dependencies and platform components are monitored and patched on a regular basis.
- Confirmed vulnerabilities are prioritised and remediated promptly.

11. Incident response

- A documented incident-response process governs detection, containment and recovery.
- Where a personal-data breach affects a customer, we notify the affected controller **without undue delay and within 72 hours**.

12. Sub-processors & vendor management

- We engage a limited set of vetted sub-processors (hosting, file storage, transactional email, payments) under GDPR-compliant contracts. The current list is published on the Sub-processors page, and changes are announced in advance.

13. Data protection & retention

- Processing is GDPR-compliant; a **Data Processing Agreement** and **TOMs** are available in this Trust Center.
- On account termination, personal data is permanently deleted within **30 days**; backups expire after their retention period.
- Data subjects can exercise their rights of access, rectification, erasure, restriction, portability and objection.

14. Personnel security

- Staff are bound by confidentiality obligations and granted access strictly on a need-to-know basis.

15. Responsible disclosure

We welcome reports from security researchers. Please contact **security@fotostudio.io**; we acknowledge reports promptly and work to remediate confirmed issues quickly. Please act in good faith and avoid accessing or modifying other users' data.

16. Contact

Security: security@fotostudio.io · General: support@fotostudio.io

> *Review note (EN): ISO 27001 / SOC 2 are certifications of the infrastructure providers (Heroku, AWS), not of Fotosoft itself — keep this attribution accurate. Confirm encryption-at-rest scope and the availability SLA with the team.*