Technical & Organizational Measures (TOMs)

Version 1

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

Technical and Organizational Measures

Measures implemented by **Fotosoft SA** (fotostudio.io) pursuant to Article 32 GDPR.

1. Confidentiality

- **Encryption in transit** via HTTPS/TLS for all connections.
- **Passwords** are stored hashed and salted, never in clear text.
- **Access control:** server access requires two-factor authentication; access is limited to authorised personnel on a need-to-know basis.
- Uploaded files are served through secure, non-public links.

2. Integrity

- Changes to records are attributable to individual user accounts.
- Hosting on infrastructure certified to **ISO 27001** and **SOC 1/2/3** standards (certifications of the hosting providers Heroku/Salesforce and AWS, not of Fotosoft).

3. Availability and resilience

- **Daily backups** with geographic redundancy.
- Target service availability of **99.9%** per year.
- 24/7 automated monitoring.

4. Security incident handling

- Documented incident-response process.
- Notification of affected controllers within **72 hours** for personal-data breaches.

5. Data minimisation and deletion

- Data is deleted within **30 days** after account termination; backups expire thereafter.
- Fotosoft does not resell user data or use it for its own commercial purposes.

> *Review note (EN): ISO 27001 / SOC 2 are certifications of the infrastructure providers (Heroku, AWS), not of Fotosoft itself — keep this attribution accurate.*