Technical-organisational measures for data security and data protection Art. 5, Art. 30 and Art. 32 GDPR

Company IT structure
The following areas are defined:

- In-house PC or server
- data backups
- internet server
- Any PC with Internet access

Principles of IT security

- Legality and Fairness
- Principle of good faith
- transparency
- earmarking
- Data minimization and economy
- data correctness
- Integrity and confidentiality
- accountability

All stored data are according to BSI standard 100-Z data of the category NORMAL. Only with pictures a deviation can occur, which is legal then however by the KUG.

Legality
Kundendaten kommen von

- existing contacts
- from the imprint of publications
- Recommendations and own research
- Photographer data is based on an existing contract.
- Images comply with the legal requirements of the KUG.

Transparency, earmarking, data minimization
is manufactured by the present description and the web page imprint and data protection.
Only data necessary for the fulfilment of the business purpose will be stored.
The websites of delosfoto GmbH are free of advertising.

Privacy

- Access control: The 3 operating rooms (server cellar, work room ground floor and office DG) are locked and only accessible for employees and visitors.
- Access authorisation: The network server is password protected, access is only possible as a special user or administrator.
- All PCs are password protected. A desktop lockout occurs after 10 minutes of non-use.
- Access authorization and separation control: Access to accounting and payroll accounting is only possible from the accounting PC in the EC workroom.
- Data backup hard disks are kept locked.
- A visitor regulation or reception control also ensures the confidentiality of all data.
- Affiliated photographers only have access to their own images.

Integrity

- Controls on the transfer of data: Suppliers and other service providers do not receive customer data.
- Encrypted connection of the contact page of the website.
- When using TeamViewer VPN is used.
- External service providers: (maintenance and support of the admin program and the website) is only provided by a reliable service provider; a confidentiality agreement has been concluded.
- Hard disks are currently not encrypted.

Availability and resilience

- Each of the PCs has a firewall and the operating system Windos7 (as of 12.07.2019) or Windows10 with Windows Defender or a virus protection program such as ESET.
- The in-house server works with Windows7 and thus also corresponds to the state of the art. The

hard disks are mirrored with Raid1.

- Fire protection is not available. Multiple data security is implemented:
  Level 1 on the server; mirrored hard disks
  Stage 2 on a NAS hidden in the operating rooms. However, images are excluded here.
  Level 3 on removable hard disks (mainly image files).
  Level 3 is doubled.
- The server on the Internet stores the data backup on a separate partition and transfers the encrypted data daily to AWS.
- The access data of the program part Uploader are stored encrypted in the program.

Control of measures

- Windows10 and Windows7 (still) are considered to be state of the art.
- Operating systems and user programs of the workstation PCs are automatically updated.
- The in-house server is updated every 3 months by an IT specialist.
- The Internet server automatically receives updates.
- Procedural changes are regularly updated in the respective procedural indexes.
- An evaluation of the technical and organizational measures must always take place when changes are made to the hardware and software equipment.
- By the end of 2019, all PCs and the server will be converted to Windows10. Older operating systems do not exist.
- **Employee training on data protection and data security takes place annually.**

Vcrapping of discarded hardware

Programs are deleted
The hardware is disposed of without a hard disk as ordinary electrical waste.
Hard disks are removed and made unusable as shown in the picture on another device: