Technisch-Organisatorische-Maßnahmen zur Datensicherheit und *Datenschutz*
Art. 5, Art. 30 und Art. 32 DSGVO

Struktur der Firmen-IT
Definiert sind folgende Bereiche:
- Hauseigene PC bzw. Server
- Datensicherungen
- Internetserver
- Jeder PC mit Zugang zum Internet

Grundsätze der IT-Sicherheit
- Rechtmäßigkeit und Fairness
- Grundsatz Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung und-sparsamkeit
- Datenrichtigkeit
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Alle gespeicherten Daten sind nach BSI-Standard 100-Z Daten der Kategorie NORMAL. Nur bei Bildern kann eine Abweichung vorkommen, die dann jedoch durch das KUG rechtmäßig sind.

Rechtmäßigkeit
Kundendaten kommen von
- bestehenden Kontakten
- aus dem Impressum von Publikationen
- Empfehlungen und eigener Recherche

Fotografendaten basieren auf einem bestehenden Vertrag.
Bilder entsprechen den gesetzlichen Vorgaben des KUG.

Transparenz, Zweckbindung, Datenminimierung
wird hergestellt durch die vorliegende Beschreibung und die Webseite Impressum und Datenschutz.
Es werden nur Daten gespeichert, die zur Erfüllung des Betriebszweckes notwendig sind.
Die Webseiten der delosfoto GmbH sind werbefrei.

Vertraulichkeit
- Zugangskontrolle: Die 3 Betriebsräume (Serverkeller, Arbeitsraum EG und Büro DG) sind verschlossen und nur für MA und Besucher zugänglich.
- Zugangsberechtigung: Der Netzwerkserver ist Passwortgeschützt, ein Zugang ist nur als spezieller Nutzer bzw. Administrator möglich.
- Alle PCs sind Passwortgeschützt. Eine Desktopsperre erfolgt nach 10-minütiger Nichtbenutzung.
- Zugangsberechtigung und Trennungskontrolle: Zugriff auf Buchführung und Lohnabrechnungen ist nur vom Buchführungs-PC im Arbeitsraum EG aus möglich.
- Festplatten der Datensicherung werden verschlossen aufbewahrt.
- Eine Besucherregelung bzw. Empfangskontrolle sichert ebenfalls die Vertraulichkeit aller Daten.
- Angeschlossene Fotografen haben nur Zugriffsberechtigung zu ihren eigenen Bildern.

Integrität
- Weitergabekontrolle: Lieferanten und andere Dienstleiter erhalten keine Kundendaten.
- Verschlüsselte Verbindung der Kontaktseite der Webseite.
- Bei dem Einsatz von TeamViewer kommt VPN zum Einsatz
- Externe Dienstleister: (Wartung und Support des Admin-Programms und der Webseite) erfolgt nur durch einen zuverlässigen Dienstleister; eine Vertraullichkeitsvereinbarung ist geschlossen.
- Festplatten sind zur Zeit nicht verschlüsselt.

Verfügbarkeit und Belastbarkeit
- Jeder der PCs verfügt über Firewall und das Betriebssystem Windos7 (Stand 12.07.2019) bzw. Windows10 mit dem Windows Defender oder ein Viren-Abwehrprogramm wie ESET.

- Der Hauseigene Server arbeitet mit Windows7 und entspricht damit ebenfalls dem Stand der Technik. Die Festplatten sind gespiegelt mit Raid1.
- Ein Brandschutz ist nicht verfügbar. Implementiert ist eine mehrfache Datensicherheit:
  Stufe 1 auf dem Server; gespiegelte Festplatten
  Stufe 2 auf einem in den Betriebsräumen versteckten NAS. Hier sind jedoch Bilder ausgeschlossen.
  Stufe 3 auf Wechselfestplatten (vor allem Bilddateien).
  Stufe 3 ist doppelt vorhanden.
- Der Server im Internet speichert die Datensicherung auf einer gesonderten Partition und überträgt die Daten verschlüsselt täglich an AWS.
- Die Zugangsdaten des Programmteiles Uploader sind verschlüsselt im Programm gespeichert.

Kontrolle der Maßnahmen

- Windows10 und Windows7 (noch) gelten zur Zeit als Stand der Technik.
- Betriebssysteme und Anwenderprogramme der Arbeitsplatz-PCs erhalten automatisch Updates.
- Der Hauseigene Server wird in 3-monatigen Abständen durch eine IT-Fachkraft aktualisiert.
- Der Internet-Server erhält automatische Updates.
- Verfahrensänderungen werden in den jeweiligen Verfahrensverzeichnissen regelmäßig aktualisiert.
- Eine Evaluierung der technisch-organisatorischen-Maßnahmen muss immer stattfinden bei Änderungen der Hard- und Software-Ausstattung.
- Bis Ende 2019 erfolgt die Umrüstung aller PC und des Servers auf Windows10. Ältere Betriebssysteme existieren nicht.
- **Eine Mitarbeiterschulung zu Datenschutz und Datensicherheit findet jährlich statt.**

Verschrottung ausgemusterter Hardware

Programme werden gelöscht
Die Hardware wird ohne Festplatte als gewöhnlicher Elektroschrott entsorgt
Festplatten werden ausgebaut und wie im Bild an einem anderen Gerät gezeigt unbrauchbar gemacht: