

Was ist zu tun?

Ich bin FD und Datenschutz ist mir wichtig.

- Informationspflicht (Datenschutzerklärung auf der Homepage)
- Ordner anlegen für Datenschutzerklärung, Verarbeitungsverzeichnis, Auftragsverarbeiter, Mitarbeiter Einwilligungen, Kunden Einwilligungen, Aufzeichnung über Auskünfte (Logbuch)
- Verarbeitungsverzeichnis erstellen
- Auftragsverarbeiter kontaktieren für Zusatzvertrag (wenn möglich)
- Mitarbeiter Einwilligung einholen
- Zugriff auf PC/Ordner schützen und nur Befugten Zugang erlauben
- Datensicherung (mind. alle 6 Tage komplette Daten) einrichten
- Betriebssystem (PC, Virusprogramm, Homepage-System) immer aktuell halten
- Homepage mit SSL verschlüsseln (https://) - grünes Schloss

DSGVO fit ;)

Ich bin FD und Datenschutz Bürokratie interessiert mich nicht

1. Datenschutzerklärung auf der Homepage
2. Bei Auskunftspflicht habe ich 1 Monat Zeit um alles zu regeln.

Checklist bei Auskunft:

Identität: Inhaberschaft mit Lichtbildausweis bestätigen lassen.

Zeitraum: Innerhalb von 1 Monat reagieren - sowohl bei der Auskunft als auch intern um DSGVO-fit zu werden.

Was muss ich bei Neukunden machen?

- Bei direkten Kontakt - Datenschutzerklärung mitgeben - muss nicht unterschrieben werden.
- Bei telefonischen Kontakt - Verweis auf die Homepage mit der Datenschutzerklärung
- Bei E-Mail-Kontakt - Link mit der Datenschutzerklärung in der Signatur
- Einwilligung einholen für Marketingmaßnahmen (zukünftige Telefonate, E-Mails, Postsendungen, etc.)

Was muss ich bei Altkunden machen?

Link mit Datenschutzerklärung in der E-Mail-Signatur, bzw. Hinweis das die Datenschutzerklärung im Büro aufliegt.

Checklist DSGVO

Daten:	Welche personenbezogene Daten werden verarbeitet?
Datensicherheit:	Welche Maßnahmen werden gesetzt um die Daten zu schützen? Wer hat Zugriff auf diese Daten? Wer darf oder kann Daten verändern, berichtigen, löschen? Werden die Daten weitergeleitet? Wenn ja, an wen? EU oder Drittland? Ist mein Betriebssystem aktuell, Virenprogramm aktuell, Homepagesystem aktuell? Können die Daten wiederhergestellt werden, nach einem Verlust?
Daten Minimierung:	Wann können die Daten gelöscht werden? Werden nur die Daten verwendet lt. Zweck?
Rechtsgrundlage:	Ist eine Einwilligung vorhanden, ist ein Vertrag vorhanden?
Informationspflicht:	Wird auf die Verwendung von Daten hingewiesen? Homepage, Newsletter, Mitarbeiter Erklärung, Info-Aushang, etc.
Rechenschaftspflicht:	Ist alles dokumentiert was ich getan habe? Haben Verarbeiter einen Vertrag zugesandt?