

C H E C K L I S T E zur D S G V O

für Steinmetzbetriebe der Bundesinnung der Bauhilfsgewerbe

Die 10 wichtigsten Schritte:

1. Feststellung des Ist-Zustandes

Erheben Sie in Ihrem Betrieb

wer (= ihr Unternehmen)

welche Daten (= „fremde“ personenbezogene Daten, wie Daten ihrer Mitarbeiter, Kunden...)

wozu verarbeitet (= Zweck der Datenverarbeitung, zB Gehaltsauszahlung, Newsletter, etc.)

und

aufgrund welcher Rechtsgrundlage (= Vertragserfüllung, Einwilligung, etc.)

wo und wie lange diese Daten gespeichert bzw. aufbewahrt werden

und

an wen diese Daten weitergegeben werden (=Datenempfänger, wie etwa Steuerberater, Bank, Übermittlung an Drittstaaten, etc).

2. Erstellung einer Dokumentation der Verarbeitungsvorgänge

Erarbeiten Sie Verfahrensverzeichnisse, gegebenenfalls unter zu Hilfenahme von Mustern.

Das Verfahrensverzeichnis unterliegt keinen Formvorschriften. Um den inhaltlichen

Vorgaben zu entsprechen, empfehlen wir jedoch ein Muster zu verwenden bzw. bei der

Erstellung sich daran zu orientieren. <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html>

3. Verträge mit Auftragsverarbeitern

Übermitteln Sie Daten an Dritte, damit diese „ihre“ Daten weiterverarbeiten, sollten Sie

bestehende Verträge mit ihren Auftragsverarbeitern (Steuerberater, Lohnverrechner,

Cloud-Anbieter, etc...) überarbeiten bzw. evaluieren Sie, ob etwaige Neuabschlüsse sinnvoll

sind. Den Mustervertrag finden sie unter <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html>

4. Bestellung eines Datenschutzbeauftragten

Prüfen Sie, ob Sie verpflichtend einen Datenschutzbeauftragten bestellen müssen. Da in

Steinmetzbetrieben die Datenverarbeitung grundsätzlich keine Kerntätigkeit darstellen

sollte und üblicherweise auch kaum „sensible“ Daten (= rassische, ethnische, religiöse,

politische, weltanschauliche, genetische, biometrische, Gesundheitsdaten und Daten zum

Sexualleben) verarbeitet werden, wird in den meisten Fällen kein Datenschutzbeauftragter

benötigt werden. Es steht jedoch jedem Betrieb frei, einen solchen zu bestellen, um eine

Ansprechperson im Unternehmen für den Datenschutz zu haben.

5. Durchführung einer Datenschutz-Folgenabschätzung

Prüfen Sie, ob Sie verpflichtend eine Datenschutz-Folgeabschätzung durchführen müssen.

In Steinmetzbetrieben in aller Regel nicht notwendig, da weder „sensible“ Daten in

großem Umfang verarbeitet werden, noch die Datenverarbeitungsvorgänge ein hohes Risiko

für Betroffene mit sich bringen. Auch ohne Verpflichtung steht es Ihnen frei, eine solche durchzuführen.

6. Informationspflichten und Betroffenenrechte

Wenn Sie Daten erheben, haben Sie die Betroffenen in Form einer Datenschutzerklärung darüber zu informieren. Überprüfen Sie, ob Sie die vorgesehenen Informationspflichten erfüllen und stellen sich sicher, dass Sie die Betroffenenrechte wahren.

<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html>

7. Meldung etwaiger Verstöße

Erstellen Sie oder besorgen Sie sich ein Muster für die Meldung von Datenschutzverletzungen. <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html>

8. Prüfung und Anpassung der bisher verwendeten Formulare

Evaluieren Sie die bislang verwendeten Formulare (z.B. Aufklärungs- und Einwilligungsbögen sowie Zustimmungserklärungen in AGB und auf Ihren Webseiten).

9. Sicherheitsmaßnahmen

Überprüfen und passen Sie bestehende technische und organisatorische Sicherheitsmaßnahmen an und dokumentieren Sie diese im Verfahrensverzeichnis. Überlegen Sie sich ein Kontrollsystem. Weitere Infos zur IT-Sicherheit unter <https://www.wko.at/service/innovation-technologie-digitalisierung/it-sicherheit-datensicherheit.html>

10. Mitarbeiterschulungen

Führen Sie Mitarbeiterschulung durch und schließen Sie eine schriftliche Vereinbarung mit den Mitarbeitern ab.

Weitere Informationen: www.wko.at/Datenschutz und www.wko.at/datenschutzservice

Verarbeitungsverzeichnis

- Wer - verarbeitet Daten
- Was - wird verarbeitet (Datenkategorien)
- Warum - verarbeite ich (Rechtsgrund)
- Wozu - verarbeite ich (Zweck der Verarbeitung)
- Wohin - übermittle ich die Daten
- Wie lange - speichere ich die Daten
- + **Datensicherungsmaßnahmen** (technisch/organisatorisch)

DATENSCHUTZERKLÄRUNG

- Name/Kontaktdaten
- Erhobene Daten (nach Kategorien)
- Rechtsgrundlage
- Zweck
- Übermittlungsempfänger
- Speicherdauer
- Info über Betroffenenrechte
- Widerrufsrecht bei Einwilligung

Betroffenenrechte: Recht auf...

- Auskunft (binnen 1 Monats)
- Berichtigung
- Einschränkung/Löschung
- Widerspruch/Widerruf
- Datenübertragbarkeit
- Beschwerdemöglichkeit