SMARACIS

Checkliste Datenschutzgrundverordnung (DSGVO)

Die einfache & praxisbewährte Checkliste

Stand: 25.06.2018

Einleitung

Mit dieser Checkliste erfahren Sie alles was Sie **unbedingt tun müssen**, um der DSGVO zu genügen.

Diese Checkliste ist speziell auf Selbstständige und Kleinunternehmer ausgerichtet – und daher so **einfach** wie möglich gestaltet.

Die Checkliste zeigt Ihnen die wichtigsten Schritte zur praktischen Umsetzung der neuen Datenschutz-Grundverordnung. Sie hilft Ihnen bei der Erfüllung der notwendigen Anforderungen, um hohe Strafen durch Verletzungen der DSGVO zu vermeiden.

7 Schritte, die Sie unbedingt umsetzen müssen:

1. Beantworten Sie die wichtigsten Grundfragen
2. Erstellen Sie ein Datenverarbeitungsverzeichnis
3. Auftragsverarbeitung sicherstellen
4. Personal-Vereinbarungen treffen
5. Risiko prüfen und abschätzen
6. Sicherheits-Maßnahmen umsetzen
7. Die laufende Einhaltung der DSGVO sicherstellen

Schritt #1:
Beantworten Sie die wichtigsten Grundfragen

Beantworten Sie zuerst die wichtigsten Grundfragen.

1. Frage: Welche personenbezogenen Daten verarbeiten Sie überhaupt?

➤ Sammeln Sie alles, was Ihnen einfällt.

Tipp: Um bei der Datensammlung nichts zu übersehen, nutzen Sie folgende drei Betrachtungsperspektiven:

- *Prozesssicht: Welche Daten werden in Ihren Prozessen verarbeitet?*
- *Toolsicht: Welche Daten werden in Ihren Tools verarbeitet?*
- *Beteiligte: Wer sendet bzw. erhält die Daten?*

2. Frage: Verarbeiten Sie sensible Daten?

➤ Die folgenden Daten sind „sensibel“:

- Rassische oder ethnische Herkunft (z. B. Geburtsland)
- Religiöse, politische und weltanschauliche Überzeugungen (z. B. Religionsbekenntnis)
- Gesundheitsdaten (z. B. Krankenstände)
- Genetische oder biometrische Daten (z. B. Fingerabdruck)
- Daten zum Sexualleben oder sexueller Orientierung (z. B. Homosexualität)

3. Frage: Benötigen Sie einen Datenschutzbeauftragten?

➤ Ihr Unternehmen benötigt einen Datenschutzbeauftragten, wenn mindestens eine der folgenden Aussagen auf Ihr Unternehmen zutrifft

- Ihre „**Kerntätigkeit**“ ist die **„umfangreiche“** Verarbeitung von **sensiblen Daten** (Eine Lohnverrechnung für Ihre Mitarbeiter gehört z.B. nicht dazu, da dies nur ein Unterstützungsprozess ist.)
- Ihre „**Kerntätigkeit**“ ist die **„umfangreiche“** Verarbeitung von **strafrechtlichen Daten**
- Sie Verarbeiten **besonders heikle Daten** (z. B. Standort-Tracking)

Tipp: Sollten Sie einen Datenschutz-Beauftragten benötigen (was bei Kleinunternehmen selten der Fall ist), können Sie sich hier näher informieren, was zu tun ist:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Der-Datenschutzbeauftragt.html

Schritt #2: Erstellen Sie ein Datenverarbeitungsverzeichnis

Das Verarbeitungs-Verzeichnis ist die wohl wichtigste Aufgabe, die praktisch jedes Unternehmen in Österreich machen muss. Es gibt so gut wie keine Ausnahmen!

- **Verwenden Sie bestehende Muster und Vorlagen** von Datenschutz-Vereinen, Kammern oder Experten und passen Sie diese auf Ihr Unternehmen an.
  - WKO: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html
  - Bitkom: https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html

Tipp: Folgende Inhalte müssen abgedeckt werden:

A) **Betroffene:** Wer sind die Betroffenen (zusammengefasst in Kategorien), von denen Sie die Daten verarbeiten?

B) **Zwecke:** Wozu verarbeiten Sie die Daten?

C) **Daten-Kategorien:** Welche Daten verarbeiten Sie?

D) **Empfänger:** Wohin gehen die Daten / wer bekommt die Daten?

E) **Fristen:** Wie lange dürfen Sie die Daten aufbewahren?

F) **Rechtsgrundlage:** Dürfen Sie die Daten überhaupt verarbeiten?
Sobald eine der unten angeführten Voraussetzungen erfüllt ist, dürfen Sie die Daten verarbeiten:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die

im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

➤ Speichern Sie die Datei jedes Mal als neue Datei mit dem neuen Datum
Tipp: Die alte Datei nie überspeichern, damit Änderungen nachvollziehbar bleiben

Schritt #3: Auftragsverarbeitung sicherstellen

a) Welche Auftragsverarbeiter haben Sie?

➤ Listen Sie alle Ihre Auftragsverarbeiter auf.
(Einige Beispiele für Auftragsverarbeiter):

- IT-Dienstleister (z. B. EDV-Wartung, außer ein Zugriff auf personenbezogene Daten ist nicht möglich bzw. absolut ausgeschlossen)
- Cloud-Anbieter (z. B. für CRM-Lösungen)
- Webhoster (wenn Sie eine Website haben)
- E-Mail Anbieter
- Google (wenn Sie Google-Dienste nutzen wie z. B. Google Analytics, Adwords, Gmail, GSuite …)
- Evtl. Facebook
- Software
- …

b) Gibt es eine Auftragsverarbeitervereinbarung?

➤ Fragen Sie beim Dienstleister nach, ob er eine „Auftragsverarbeitervereinbarung“ zur Verfügung stellt *(Hinweis: Bei Google & Co. gibt es in der Regel aktualisierte Nutzungsverträge/-bedingungen oder Datenschutzerklärungen, denen zuzustimmen ist).*

➤ Verwenden Sie ansonsten Muster, passen Sie diese für Ihr Unternehmen an und schicken Sie die Vereinbarung an Ihre Dienstleister zur Unterzeichnung.

- WKO: *https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html*
- Bitkom: *https://www.bitkom.org/Bitkom/Publikationen/Begleitende-Hinweise-zu-der-Anlage-Auftragsverarbeitung.html*

➤ Schließen Sie Auftragsverarbeitervereinbarungen
Tipp: Stellen Sie sicher, dass Sie mit allen Ihren Auftragsverarbeitern einen Vertrag

haben, der den Datenschutz (laut DSGVO) regelt.

c) Sind Sie selbst Auftragsverarbeiter?

- **Wenn ja: Erstellen Sie ein Verarbeitungsverzeichnis** für alle Daten, die Sie im Auftrag des Verantwortlichen verarbeiten.
- **Wenn nein: Gehen Sie weiter zu Schritt #4.**

Schritt #4: Personal-Vereinbarungen treffen

Sollten Sie keine Mitarbeiter haben, gehen Sie weiter zu Schritt #5.

- **Erstellen Sie Personal-Vereinbarungen für Datenschutz**
  - **Datengeheimnis-Verpflichtungserklärung**
    z. B. *www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html*
  - **Datenschutzerklärung für Mitarbeiter**
    z. B. *www.wko.at/service/wirtschaftsrecht-gewerberecht/dsgvo-muster-datenschutzerklaerung-mitarbeiter.html*
  - **Nutzungsregeln der EDV** (PC, Smartphone, Telefon usw.)
    z. B.
    www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html
  - **Schriftliche Einwilligungen** (z. B. für die Veröffentlichung von Mitarbeiter-Bildern auf der Website) z. B. *https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html*

Tipp: Gleichen Sie die Infos der Personal-Vereinbarung mit dem Datenverarbeitungs-Verzeichnis ab, um sicherzustellen, dass nichts vergessen wurde.

- **Lassen Sie die Vereinbarung im Rahmen von Gesprächen und Schulungen von allen Mitarbeitern unterschreiben.**

Schritt #5: Risiko prüfen und abschätzen

a) Benötigen Sie eine Datenschutz-Folgeabschätzung?

- **Prüfen Sie, ob Sie eine Datenschutz-Folgeabschätzung benötigen**
  Sie müssen nur eine Datenschutz-Folgeabschätzung machen, wenn Ihre Datenverarbeitung ein hohes Risiko für die Rechte der betroffenen Personen darstellt.

  Tipp: Machen Sie immer eine Risikoanalyse, um festzustellen ob eine Datenschutz-

Folgeabschätzung notwendig ist.

Häufige Beispiele für ein hohes Risiko sind:

- Machen Sie **Profiling**? Das heißt, dass Sie Profile von Personen erstellen (z. B. über ihr Verhalten)
- Verarbeiten Sie **sensible Daten** oder andere **vertrauliche Daten** (z. B. Bankdaten, Standortdaten, Strafdaten, private Kommunikationsdaten …) in „**umfangreicher Art und Weise**" (viele betroffene Personen oder viele Daten …)?
- Übermitteln Sie (sensible/vertrauliche) Daten in **Drittstaaten** außerhalb der EU?
- Verwenden Sie **neue Technologien**, die ein hohes Risiko für die betroffenen Personen darstellen können? (z. B. CRM-Cloud-Lösungen für Kunden)

Mit der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), StF: *BGBl. II Nr. 108/2018* wurden Datenverarbeitungen definiert, die von der Datenschutz-Folgeabschätzung befreit sind. Die gesamte Liste finden Sie unter:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010206
Einige Beispiele sind:

- DSFA-A01: Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
- DSFA-A02: Personalverwaltung

DSFA-A03: Mitgliederverwaltung

Tipp: Sind Sie unsicher, ob eine Datenschutz-Folgeabschätzung notwendig ist, wenden Sie sich an einen Datenschutz-Experten oder an Ihren Datenschutzbeauftragten.

b) Falls notwendig, wie führen Sie eine Datenschutz-Folgeabschätzung durch?

- **Beschreiben Sie die Datenverarbeitungen genauer**
  - Verwenden Sie das Verarbeitungsverzeichnis als Grundlage
  - Genauere Beschreibung der Abläufe, wie Sie die Daten verarbeiten
  - Welche IT-Systeme und andere Mittel Sie dabei einsetzen
- **Risikoanalyse: Bestimmen und bewerten Sie das Risiko für die Betroffenen inklusive der möglichen Auswirkungen, die ein Datenverlust bzw. Datenleck zur Folge hätte.**
- **Setzen Sie Maßnahmen, um das Risiko zu vermindern**
- **Prüfen und erklären Sie, ob Sie das Risiko ausreichend senken konnten**
  Falls trotz aller möglichen Maßnahmen immer noch ein hohes Risiko besteht, müssen Sie dies der Datenschutz-Behörde mitteilen (=vorherige Konsultation), die dann über die weitere Datenverarbeitung entscheidet.

Schritt #6: Sicherheits-Maßnahmen umsetzen

- **Stellen Sie sicher, dass Sie alle Basis-Maßnahmen zum Datenschutz umsetzen**. Folgende Schritte sind z. B. für die meisten Kleinunternehmen unbedingt notwendig:

- **Löschregeln** festlegen: Löschfristen einhalten und Daten sicher löschen (z. B. Papier in den Shredder, alte CDs oder Festplatten vernichten)
- **Daten** auf den aktuellsten Stand bringen (z. B. Kundendaten)
- **Sichere Passwörter** verwenden (bei Software, PC-Benutzerkonten, mobilen Geräten, Internet-Seiten …)
- **Verschlüsselung** einsetzen (bei E-Mails, Smartphones, USB-Sticks usw.)
- Stets die **Software aktualisieren** (z. B. Virenschutz, Internetbrowser …)
- **Datensicherung** (Backups) regelmäßig durchführen, Notfälle testen und Sicherungskopien auch an anderem Ort aufbewahren
- **WLAN** absichern (starke Verschlüsselung, Passwörter usw.)
- **Räumliche** Maßnahmen prüfen (z. B. Zutrittskontrolle, Brandschutz usw.)
- **Clear Desk**: Schreibtisch leeren (nichts herumliegen lassen) und Bildschirm sperren (sobald Sie den PC verlassen)
- **Weitere Maßnahmen** finden Sie z. B. im Sicherheitshandbuch der WKO: *https://www.wko.at/site/it-safe/sicherheitshandbuch.html*

➤ **Setzen Sie die wichtigsten Website-Maßnahmen um** wie z.B.:

- Erstellen Sie eine **Datenschutzerklärung**
- **Veröffentlichen** Sie die Datenschutzerklärung als eigene Seite auf Ihrer Website (nicht unter dem Impressum / den AGB, sondern wirklich als eine eigene Seite)
- **Informieren** Sie die Betroffenen über Ihre Datenschutzerklärung (z. B. Link in E-Mail Signatur, Dokumenten usw.)
- Integrieren Sie auf Ihrer Website einen **Hinweis-Banner** für Ihre Datenschutzerklärung und die Verwendung von Cookies
- Stellen Sie **Einwilligungen** sicher (z. B. eindeutige Zustimmung für E-Mail Versand)
- **Verschlüsselung** der Website („https“ statt „http“)

➤ **Schreiben Sie alle Ihre Maßnahmen in Ihr Datenverarbeitungsverzeichnis.**

➤ **Prüfen Sie, ob Sie alle DSGVO-Grundsätze einhalten.** Falls Sie noch nicht alle Grundsätze einhalten, setzen Sie weitere Maßnahmen.

Schritt #7:
Die laufende Einhaltung von Datenschutz sicherstellen

Bitte bedenken Sie: Datenschutz ist keine einmalige Aufgabe, sondern eine regelmäßige Arbeit, die immer berücksichtigt werden muss (z. B. genauso wie Steuern zahlen oder die Buchhaltung erledigen). Folgende Aufgaben sollten Sie jedenfalls regelmäßig durchführen:

➤ Die **Datenschutz-Grundsätze** langfristig einhalten und jederzeit bereit sein dies zu **beweisen** *(Achtung: Sie müssen der Datenschutz-Behörde jederzeit nachweisen können, dass Sie alle Datenschutz-Grundsätze einhalten)*

➤ Ihr **Daten-Verarbeitungsverzeichnis** laufend aktualisieren und erweitern

- Ihre **Auftragsverarbeiter** prüfen (Eine Kontrolle ist zwar nicht vorgeschrieben, doch eine regelmäßige Prüfung ist ratsam, weil auch Sie für Datenschutz-Verletzungen Ihres Auftragsverarbeiters voll haften.)
- Ihr **Personal** regelmäßig schulen und auf dem aktuellsten Stand halten
- Regelmäßig prüfen, ob die **Datenschutz-Folgeabschätzung** aktuell ist
- Ihre **Datenschutz-Maßnahmen** regelmäßig checken und verbessern
- Mit der **Datenschutz-Behörde** „zusammenarbeiten“
    - Im Falle eines Datenlecks Meldung an die Datenschutzbehörde durchführen („Data Breach Notification“) *www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html*
    - Alle Datenschutz-Dokumente gut auffindbar zusammenstellen, um sie jederzeit der Datenschutz-Behörde übermitteln zu können

Impressum

SMARACIS GmbH

Gesellschaft mit beschränkter Haftung

Unternehmensberatung, Buchhaltung und Informationstechnologie (UBIT)

Adresse: 1160 Wien, Hasnerstrasse 110, Österreich

Tel: +43 676 5462298

E-Mail: office@smaracis.com

Mitglied der WKO, Fachgruppe UBIT; Arge ProEthik

Geprüfter Datenschutzexperte: Stefan Weigelhofer

Disclaimer

Sämtliche Inhalte wurden mit größtmöglicher Sorgfalt zusammengestellt, erfolgen jedoch ohne Gewähr. Sie stellen keine Beratungsleistung welcher Art auch immer dar und können eine entsprechende Beratung nicht ersetzen. Insbesondere deswegen wird keine Haftung hinsichtlich Richtigkeit, Vollständigkeit und Aktualität der Informationen (einschließlich des Verweises auf andere Quellen) übernommen. Der Verfasser schließt jegliche Haftung aus, sei es aus Vertrag, Delikt (inklusive Fahrlässigkeit) und/oder jeder anderen Rechtsgrundlage, für Verluste oder Schäden, einschließlich entgangenen Gewinns oder sonstiger direkter oder indirekter Folgeschäden, welche durch den Gebrauch oder das Vertrauen in die in dieser Unterlage zur Verfügung gestellten Informationen oder einer etwaigen Nichtberücksichtigung bestimmter Informationen entstehen.