In 10 Schritten zur DSGVO – Die 7 wichtigsten TO DOs

Die Fragen

- Wie fange ich an?
- Wie finde ich mich auf wko.at zurecht?
- Welche Unterstützung gibt es von der WKNÖ?

wurden im Workshop „*Kurz und Kompakt: Das 1x1 der Datenschutz-Grundverordnung*“ geklärt.

Wir haben die wichtigsten Umsetzungsschritte nochmals in Form eines Schnell-Überblicks zusammengestellt, der Sie in 10 Schritten durch die wesentlichen Bestimmungen führt und in 2 Anhängen einerseits ganz konkret die wichtigsten Umsetzungsschritte (7 TO-DOs) nennt, andererseits das „Herzstück“ jeder Datenverarbeitung, die sogenannten „Rechtsgrundlagen“ erklärt. Bei jedem Schritt finden Sie zusätzlich weitere Informationen direkt auf wko.at.

Hinweis: Jeder der folgenden 10 Schritte kann in beliebiger Reihenfolge bzw. auch einzeln gesetzt werden, um gezielt bestimmte Inhalte aus dem Workshop zu wiederholen oder zu vertiefen. Die Abfolge der 10 Schritte ist so gewählt, dass die Informationen vom Allgemeineren immer mehr ins Speziellere gehen. Als Umsetzungsschritte wurden jene ausgewählt, die jedenfalls gesetzt werden müssen. Abhängig von der Situation im Einzelfall können auch noch weitere Umsetzungsschritte (z.B. Bestellung eines Datenschutzbeauftragten, Durchführung einer Datenschutz-Folgenabschätzung) erforderlich sein.

In 10 Schritten zur DSGVO

1. **VORFRAGE: Verarbeiten Sie personenbezogene Daten?**

   Wahrscheinlich lautet Ihre Antwort: Ja! Kundendaten, Mitarbeiterdaten, alle Daten, die einen Bezug oder Rückschluss zu einer Person (die DSGVO spricht von „Betroffenen“) zulassen, sind personenbezogene Daten. Das Medium ist dabei egal, auch eine händisch sortierte Visitenkartensammlung stellt in der Regel eine Verarbeitung personenbezogener Daten dar.

   Nähere Infos dazu finden Sie hier:

   https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-bin-ich-betroffen-faq.html

2. **VORFRAGE: Verarbeiten Sie die personenbezogenen Daten der Betroffenen rechtmäßig?**

   Diese Frage wird Sie bei der Umsetzung immer wieder beschäftigen. Hier nur ganz kurz worum es geht: Sie benötigen für jede Datenverarbeitung einen sogenannten „Rechtsgrund“ (von der DSGVO vorgegeben) und einen „Verarbeitungszweck“ (von Ihnen für jede Datenverarbeitung zu definieren).

   Nähere Informationen finden Sie hier sowie im Anhang 1; machen Sie sich aber zuerst mit den anderen Schritten vertraut:

   https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html

3. WEBINAR

Verschaffen Sie sich – und allenfalls auch Ihren Mitarbeiterinnen und Mitarbeitern - einen Überblick und besuchen Sie unser Webinar mit weiterführenden FAQs:

https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/webinar-datenschutz-jetzt-neu-angehen.html

4. ONLINE-RATGEBER

Spielen Sie unseren Online-Ratgeber durch. Der Ratgeber ist vollkommen anonym und hilft Ihnen, aus dem umfangreichen Angebot auf wko.at jene Informationen herauszufiltern, die für Sie wesentlich sind:

https://dsgvo.wkoratgeber.at/

5. TO-DOs

Durch den Workshop und den Online-Ratgeber haben Sie einen Überblick darüber, wo Handlungsbedarf besteht. Die wichtigsten Punkte, die so gut wie immer umgesetzt werden müssen, finden Sie hier, Details im Anhang 2:

5.1. VERARBEITUNGSVERZEICHNIS (VERFAHRENSVERZEICHNIS) erstellen

5.2. RISIKOANALYSE durchführen

5.3. DATENSICHERHEITS-MASSNAHMEN überlegen

5.4. INFORMATIONSPFLICHTEN (DATENSCHUTZERKLÄRUNG) umsetzen

5.5. GEHEIMHALTUNGSVERPFLICHTUNG FÜR MITARBEITER abschließen

5.6. UMGANG MIT DEN BETROFFENENRECHTEN überlegen

5.7. AUFTRAGSVERARBEITER-VERTRÄGE kontrollieren oder abschließen

6. UMSETZUNGSHILFEN

Eine Zusammenstellung aller Unterstützungsmaßnahmen der WKO für die Umsetzung finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html

7. EXPERTEN FINDEN

Manchmal wird es sich nicht vermeiden lassen, bei der Umsetzung Experten heranzuziehen. Das muss nicht immer gleich ein Rechtsanwalt sein. Wir haben für Sie eine Liste geprüfter niederösterreichischer Unternehmen, die Ihnen bei der Umsetzung helfen können:

https://www.wko.at/service/noe/wirtschaftsrecht-gewerberecht/datenschutzexperten-noe.html

8. NACHLESE

Manchmal ist ein Buch immer noch das beste Medium, um sich mit einem neuen Thema vertraut zu machen. Wir haben für Sie alle Infos auch in Buchform kostengünstig zusammengestellt. Bestellmöglichkeit:

https://webshop.wko.at/datenschutzanpassungsgesetz-2018.html

Alle Infos in aktuellster Form finden Sie auf wko.at:

https://wko.at/Datenschutz.

9. WENN ETWAS PASSIERT IST: MELDUNG VON DATENSCHUTZ-VERLETZUNGEN

Wenn eine Datenschutz-Verletzung (Datenverlust, Datendiebstahl, Datenmissbrauch) erfolgt ist, ist dies der Datenschutzbehörde binnen 72 h melden. In vielen Fällen sind auch die Betroffenen zu informieren.

Informationen und Muster (bearbeitbar im .docx-Format und als ausgefülltes Beispiel im .pdf-Format) finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Meldung-von-Datenschutzve.html

10. WAS NICHT MEHR ALLE UNTERNEHMEN BETRIFFT: DATENSCHUTZ-BEAUFTRAGTER; DATENTRANSFER IN DRITTSTAATEN

Zur Sicherheit informieren Sie sich zum Abschluss noch, ob Sie eventuell einen Datenschutz-Beauftragten benötigen (dies wird nur in Ausnahmefällen notwendig sein) und überlegen Sie, ob Sie Daten an Drittstaaten (außerhalb der EU) übertragen (z.B. auch in Clouds):

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

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Internationaler-Datenverk.html

Alle Infos inklusive aktueller Webinare, Infoveranstaltungen und weiterführender Brancheninformationen zur DSGVO finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html

Anhang 1: Überblick über die wichtigsten Rechtsgründe und Grundsätze der DSGVO:

a. **Die Verarbeitung ist für Vertragserfüllung notwendig** (Beispiel: Adressdaten des Kunden zwecks Zustellung).

b. **Die Verarbeitung ist für Erfüllung einer rechtlichen Verpflichtung notwendig** (Beispiel: Lohnverrechnung).

c. **Lebenswichtiges Interesse des Betroffenen / öffentliches Interesse**.

d. **Berechtigtes Interesse** des Verantwortlichen oder eines Dritten, sofern nicht Interessen des Berechtigten überwiegen (Beispiel: Marketingmaßnahmen; **Achtung:** Für E-Mail-Werbung gibt es speziellere Vorschriften im Telekommunikationsgesetz TKG).

e. **Einwilligung des Betroffenen**. Diese ist dann erforderlich, wenn keiner der anderen Rechtsgründe herangezogen werden kann. (Achtung: Die Einwilligung darf nicht mit anderen Vertragserklärungen gekoppelt sein – sogenanntes „Koppelungsverbot" - und es dürfen keine vorangekreuzten Checkboxen verwendet werden – „opt in" statt „opt out").

   Nähere Informationen zur Einwilligungserklärung finden Sie hier:

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

Zusätzlich sind noch weitere Grundsätze zu beachten wie insbesondere

- **Transparenz und Fairness**

  Die Betroffenen müssen über die sie betreffenden Verarbeitungen informiert sein; siehe TO-DO 4 „Informationspflichten (Datenschutzerklärung)"

- **Datenminimierung, Speicherbegrenzung und Datenrichtigkeit**

  Daten müssen korrekt sein, dürfen nur in dem Umfang und so lange gespeichert werden, wie diese zur Erfüllung des Verarbeitungszwecks erforderlich ist.

  Anhaltspunkte für zulässige Speicherfristen finden Sie hier:

  https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html

- **Integrität und Vertraulichkeit**

  Es müssen abhängig vom bestehenden Risiko (siehe TO-DO 2 „Risikoanalyse") angemessene Datensicherungsmaßnahmen gegen Datenmissbrauch und

  unbefugten Zugriff gesetzt werden (siehe TO-DO 3 „Datensicherheits-Maßnahmen"). Nähere Informationen zu Datensicherungsmaßnahmen finden Sie hier: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Datensicherheit-und-Daten.html

  Alle Infos zu den Rechtsgründen und den Grundsätzen finden Sie hier: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Grundsaetze-und-Rechtmaes.html

Anhang 2: Die 7 wichtigsten TO-DOs kurz erklärt:

Durch den Workshop haben Sie einen Überblick darüber, wo Handlungsbedarf besteht. Die wichtigsten Punkte, die so gut wie immer umgesetzt werden müssen, sind:

1. **VERARBEITUNGSVERZEICHNIS (VERFAHRENSVERZEICHNIS)**

   Erstellen Sie ein Verzeichnis der in Ihrem Betrieb eingerichteten Datenverarbeitungen. Das Verarbeitungsverzeichnis (oder Verfahrensverzeichnis; beide Begriffe meinen dasselbe) dient zur betriebsinternen Dokumentation Ihrer Datenverarbeitungen und muss im Falle eine Kontrolle der Datenschutzbehörde vorgelegt werden können. Formvorschriften gibt es dafür nicht, wohl aber bestimmte Mindestinhalte. Informationen finden Sie hier:

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

   Achtung! Die Ausnahme von der Erstellung eines Verarbeitungsverzeichnisses für Betriebe mit weniger als 250 Mitarbeiter ist in der Praxis kaum anwendbar, weil sie nur auf „gelegentliche" (nicht regelmäßige) Datenverarbeitungen anwendbar ist.

   Muster (bearbeitbar im .docx-Format und als ausgefülltes Beispiel im .pdf-Format) finden Sie hier:

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

2. **RISIKOANALYSE**

   Im Verarbeitungsverzeichnis können Sie auch das Ergebnis der Risikoanalyse dokumentieren. Dabei handelt es sich um Ihre Einschätzung des Risikos für Betroffene in Folge von Datenverlust, Datenmissbrauch oder Datendiebstahl. Eine darüber hinausgehende sogenannte „Datenschutz-Folgenabschätzung" wird in den meisten Fällen nicht erforderlich sein, da diese nur bei einem „besonders hohen Risiko" erforderlich ist. Informationen und wann zusätzlich zur Risikoanalyse eine Datenschutz-Folgenabschätzung erforderlich ist, finden Sie hier:

   https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung-datenschutz-folgenabschaetzu.html

   Eine Checkliste zur Datenschutz-Folgenabschätzung finden Sie hier:

   https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

3. **DATENSICHERHEITS-MASSNAHMEN**

   Informationen finden Sie hier:

   https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Datensicherheit-und-Daten.html

4. INFORMATIONSPFLICHTEN (DATENSCHUTZERKLÄRUNG)

Während das Verarbeitungsverzeichnis insbesondere der Datenschutzbehörde gegenüber betriebsintern als Dokumentation erstellt werden muss, richten sich die Informationspflichten nach außen: Die „Betroffenen“ (jene Personen, deren Daten verarbeitet werden) müssen ebenfalls informiert werden. Nähere Informationen finden sie hier:

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

Damit Sie in der „Datenschutzerklärung“ keine Pflichtinformation vergessen, unterstützt Sie unser Online-Ratgeber bei der Erstellung der Datenschutzerklärung - wiederum völlig anonym:

https://dsgvo-informationsverpflichtungen.wkoratgeber.at/

5. GEHEIMHALTUNGSVERPFLICHTUNG FÜR MITARBEITER

Wenn Sie Mitarbeiter beschäftigen, müssen Sie Ihre Mitarbeiter zur Wahrung des Datengeheimnisses verpflichten. Muster (bearbeitbar im .docx-Format und als ausgefülltes Beispiel im .pdf-Format finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html

6. BETROFFENENRECHTE

Nicht nur die Datenschutzbehörde, auch Betroffene (Personen, deren personenbezogene Daten Sie verarbeiten) haben Rechte, zum Beispiel das Recht auf Löschung („Recht, vergessen zu werden“), Recht auf Auskunft, Recht auf Richtigstellung etc. Stellen Sie sicher, dass sie binnen der gesetzlichen Frist eines Monats diesen Ansprüchen nachkommen können.

Einen Überblick finden Sie hier:

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

Tipps, wie Sie im Fall der Fälle vorgehen können, finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflicht-zur-Berichtigung.html

Ein Muster für die Erledigung eines Auskunftsbegehrens (bearbeitbar im .docx-Format) finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-musterschreiben-auskunftserteilung.html

7. AUFTRAGSVERARBEITER-VERTRÄGE

Wenn Sie personenbezogene Daten zur Verarbeitung in Ihrem Auftrag an externe Dienstleister (z.B. zur Lohnverrechnung) weitergeben, benötigen Sie mit diesen Dienstleistern sogenannte „Auftragsverarbeiter-Verträge“. Diese müssen bestimmte Mindestinhalte aufweisen. Muster (bearbeitbar im .docx-Format und als ausgefülltes Beispiel im .pdf-Format) finden Sie hier:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html