****

Leitfaden zur EU-Datenschutzgrundverordnung in einem Tischlereibetrieb

Praxisorientierte Umsetzung anhand von zwei Beispielbetrieben

Inhaltsverzeichnis

[Einleitung 3](#_Toc525734096)

[Was ist die EU-Datenschutzgrundverordnung? 4](#_Toc525734097)

[Die wesentlichen Bestimmungen der DSGVO auf einen Blick 4](#_Toc525734098)

[Die für sie wichtigsten Artikel im Kurzüberblick 4](#_Toc525734099)

[**Begriffsdefinitionen** 6](#_Toc525734100)

[Personenbezogene Daten 6](#_Toc525734101)

[Besondere Kategorien personenbezogener Daten „sensible Daten“ 6](#_Toc525734102)

[**Die Datenschutzgrundverordnung und Ihr Unternehmen** 8](#_Toc525734103)

[Kategorie Rot – absolut notwendig! 9](#_Toc525734104)

[Datenverarbeitungsverzeichnis – Der Brandschutzplan für Ihre Daten 9](#_Toc525734105)

[Prozessablauf Betroffenenrechte 9](#_Toc525734106)

[Kategorie Gelb – dringend empfohlen! 10](#_Toc525734107)

[Datenschutzerklärung – Die Informationsmöglichkeit für Betroffene 10](#_Toc525734108)

[Verträge zur Auftragsdatenverarbeitung 10](#_Toc525734109)

[Verpflichtungserklärung zur Wahrung von Datengeheimnissen 10](#_Toc525734110)

[Kategorie Grün – empfohlen! 12](#_Toc525734111)

[Data Breach Protokoll und Notification 12](#_Toc525734112)

[Muster Erteilung einer Auskunft 12](#_Toc525734113)

[IT-Dokumentation 12](#_Toc525734114)

[Schulungsunterlagen 13](#_Toc525734115)

# Einleitung

Ohne Computer und Informations-Technologie geht in einem Unternehmen heutzutage gar nichts mehr. Alle Daten laufen über das Netzwerk, den Server oder die Cloud und
sind jederzeit von jedem abrufbar. So weit – so gut. Und jetzt kommt das große ABER: Wie sicher sind Ihre Daten? Vor allem die sensiblen! Um dem Datendiebstahl- und Missbrauch einen Riegel vorzuschieben, trat am 25. Mai 2018 die Datenschutz-Grundverordnung EU-weit in Kraft. Und diese DSGVO regelt auch, wie in Zukunft personenbezogene und vertrauliche Kunden-Daten handzuhaben sind. Denn jeder Kunde hat das Recht, dass seine Daten vertraulich behandelt werden und nicht in falsche Hände geraten können.

Gehen Daten in Zukunft dennoch verloren, oder werden gestohlen, dann gibts es ab Mai 2018 eine Meldepflicht an die Datenschutzbehörde.

Dieser Leitfaden soll Ihnen zeigen, wie Sie die Datenschutzgrundverordnung in Ihrem Unternehmen umsetzen können.

Hinweis: Die verwendeten Dokumente stammen von der WKO-Webseite ([www.wko.at](http://www.wko.at))

Disclaimer:Dieser Praxisorientierte Leitfaden ersetzt keine Rechtsberatung. Er soll Tischlereibetrieben aber helfen den komplexen DSGVO-Dschungel rasch und einfach zu durchschauen, um die notwendigen Schritte für den eigenen Betrieb einleiten zu können.

# Was ist die EU-Datenschutzgrundverordnung?

Die EU-DSGVO wurde vom Europäischen Parlaments und Rat zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zur Regelung des freien Datenverkehrs kundgemacht.

Die Datenschutz-Grundverordnung trat am 25. Mai 2018 in Kraft.

Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume.

Zur Durchführung dieser Öffnungsklauseln und Spielräume wurde in Österreich das „Datenschutz-Anpassungsgesetz 2018“, eine Novelle des DSG 2000 (künftig: DSG), beschlossen.

# Die wesentlichen Bestimmungen der DSGVO auf einen Blick

* Es gelten für die Art und Weise, wie Personendaten bearbeitet werden dürfen, weiterhin die bisherigen Bearbeitungsgrundsätze: So ist besonders der Grundsatz der Transparenz, der Zweckbindung und der Verhältnismäßigkeit hervorzuheben.
* Jede Datenbearbeitung erfordert die Einwilligung der Betroffenen oder einen anderen Rechtfertigungsgrund.
* Betroffene haben umfangreiche Rechte, so namentlich auf Auskunft, auf Rückgabe übergebener Daten in elektronischer Form, auf Korrektur und Vervollständigung, auf Löschung und Weitermeldung des Löschbegehrens bei veröffentlichten Daten sowie Widerspruch gegen bestimme Bearbeitungen (z.B. Direktmarketing).
* Der für eine Datenbearbeitung Verantwortliche muss belegen können, dass er den Datenschutz einhält; er und teils auch die von ihm beauftragten Stellen (Provider) unterliegen umfangreichen Dokumentationspflichten.
* Personendaten müssen durch angemessene technische und organisatorische Maßnahmen gesichert sein; eigene Datenbearbeitungen müssen so ausgestaltet sein, dass sie die Einhaltung des Datenschutzes sicherstellen (Privacy by Design) und Standard-Einstellungen, wo es solche gibt, datenschutzfreundlich sind (Privacy by Default).
* Datenschutzverstöße mit möglichen Folgen für Betroffene müssen der Behörde (72 Stunden) und bei schweren Folgen auch den Betroffenen gemeldet werden und sind protokollierungspflichtig.

### Die für Sie wichtigsten Artikel im Kurzüberblick

* Artikel 5: Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten
* Artikel 6: Rechtmäßigkeit der Verarbeitung
* Artikel 7: Bedingungen für die Einwilligung
* Artikel 12 – Artikel 23: Rechte der betroffenen Personen
* Artikel 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
* Artikel 28: Auftragsverarbeiter
* Artikel 30: Verzeichnis von Verarbeitungstätigkeiten

## **Begriffsdefinitionen**

### Personenbezogene Daten

Definitionsgemäß sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

z.B.: Name, Adresse, Geburtsdatum, Bankdaten, etc.

### Besondere Kategorien personenbezogener Daten „sensible Daten“

Das sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschafts-Zugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

z.B.: Fingerabdruck, Iris Scan, Krankengeschichte, Informationen über Straftaten etc.

**Informationspflichten und Betroffenenrechte**

Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats, zu erledigen

* Auskunftsrecht (ua. auch über geplante Speicherdauer)
* Recht auf Berichtigung
* Recht auf Löschung und auf „Vergessenwerden“
* Recht auf Einschränkung der Verarbeitung
* Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
* Recht auf Datenübertragbarkeit
* Widerspruchsrecht

**Empfänger**

Als „Empfänger“ bezeichnet die DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Von dieser Definition ist auch der Auftragsverarbeiter erfasst, d.h. auch dieser gilt als „Empfänger“.

**Verantwortlicher**

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw. die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

z.B.: Geschäftsführer, Firmeninhaber etc.

**Auftragsverarbeiter**

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

**Data Breach**

Ein Data Breach beschreibt eine Datenpannen, einen Datenverlust oder einen Datenmissbrauch.

## **Die Datenschutzgrundverordnung und**

## **Ihr Unternehmen**

In vielen Unternehmen kann die EU-Datenschutzgrundverordnung mit einfachen Schritten umgesetzt werden. Es ist aber immer von der Art und Weise und dem Umfang der Verarbeitung von personenbezogenen Daten abhängig, wieviel Zeit Sie in die Umsetzung investieren müssen.

Bei manchen personenbezogenen Daten (z.B.: Name und Anschrift Ihrer Kunden) ist das Risiko geringer als bei anderen Datensätzen (Gesundheitsdaten von Mitarbeiterinnen).

Wir haben die Dokumente für in die drei Ampelfarben ROT, GELB und GRÜN unterteilt. Die Kategorie „ROT“ sind jene Dokumente, die Sie unbedingt erstellen und ausfüllen sollten. Zur Anwendung der Dokumente in der Kategorie „ORANGE“ wird stark geraten und die die Dokumente der „GRÜNEN“ Kategorie sind Empfehlungen.

Drüber hinaus gibt es eine Vielzahl von weiteren DSGVO-Dokumenten und Prozessen, deren Umsetzung in Ihrem Unternehmen notwendig sein.

**Der Leitfaden bezieht sich auf das Minimum der notwenigen Schritte anhand der beiden Praxisprojekte.**

Die folgenden Dokumente sollten Sie ausfüllen und ergänzen sowie in einem eigenen Datenschutzordner ablegen.

Unter der Dokumenten-Beschreibung sehen Sie im gelben Kasten noch einige wichtige Kurzinformationen.

## Kategorie Rot – absolut notwendig!

### Datenverarbeitungsverzeichnis – Der Brandschutzplan für Ihre Daten

In jedem Fall sollten Sie ein Verzeichnis der Datenverarbeitungen (VDV oder Daten-verarbeitungsverzeichnis) erstellen. In diesem Verzeichnis wird beschrieben welche Datenarten, Sie mit welcher Aufbewahrungszeit und für welchen Zweck Sie in Ihrem Unternehmen aufbewahren.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Nur der Verantwortliche und auf Verlangen die zuständige Datenschutzbehörde |
| Wann muss ich dieses Dokument anlegen? | Ehestmöglich sobald Sie in Ihrem Unternehmen personenbezogene Daten erfassen oder verarbeiten.  |
| Was ist sonst noch zu beachten? |  |
| Dokumenttitel | Verfahrensverzeichnis.xls  |

### Prozessablauf Betroffenenrechte

Skizzieren Sie in diesem Dokument in wenigen Worten oder Grafiken wie Sie im Unternehmen mit dem Datenschutz in Verbindung mit den Betroffenenrechten umgehen wollen.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Nur der Verantwortliche und auf Verlangen die zuständige Datenschutzbehörde |
| Wann muss ich dieses Dokument anlegen? | Ratsam wäre eine Definition im Zuge eines Datenschutzprojektes  |
| Was ist sonst noch zu beachten? |  |
| Dokumenttitel | Prozessablauf Betroffenenrechte.docx  |

## Kategorie Gelb – dringend empfohlen!

### Datenschutzerklärung – Die Informationsmöglichkeit für Betroffene

In Ihrer Datenschutzerklärung sollte stehen welche personenbezogenen Daten Sie von Ihren Kunden und Besuchern erfassen und verarbeiten.

Es kann Datenschutzerklärungen für Kunden, Mitarbeiter, die Webseite in einzelnen Dokumenten oder in einer gesammelten Variante geben.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Mögliche Betroffene (Kunden, Besucher der Webseite, Mitarbeiter,…)  |
| Wann muss ich dieses Dokument anlegen? | Sobald Sie in Ihrem Unternehmen personenbezogene Daten erfassen oder verarbeiten bzw. Sie eine Webseite betreiben.  |
| Was ist sonst noch zu beachten? |  |
| Dokumenttitel | Datenschutzerklärung Mitarbeiter.docxDatenschutzerklärung Kunden.docxDatenschutzerklärung Webseite.docx  |

### Verträge zur Auftragsdatenverarbeitung

Wenn Sie mit anderen Unternehmen Kundendaten austauschen oder diese verfügbar machen (z.B.: Fernwartung eines EDV-Dienstleisters bei Ihrem Buchhaltungsprogramm), dann müssen Sie mit diesen Unternehmen sogenannte Auftragsdatenverarbeitungsverträge schließen.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Nur die beiden Vertragspartner bzw. auf Verlangen die zuständige Datenschutzbehörde |
| Wann muss ich dieses Dokument anlegen? | Sobald Ihr Unternehmen personenbezogene Daten an ein anderes Unternehmen weiterleitet oder den Zugriff darauf ermöglicht.  |
| Was ist sonst noch zu beachten? | Dieses Dokument sollte von beiden Verantwortlichen unterzeichnet sein. |
| Dokumenttitel | Vereinbarung zur Auftragsdatenverarbeitung.docx  |

**Eine Auflistung von Unternehmen mit denen ein ADV geschlossen werden muss, sollte sich im Verarbeitungsverzeichnis im Blatt „Datenanwendungen“ befinden.**

### Verpflichtungserklärung zur Wahrung von Datengeheimnissen

Dieses Dokument ist für Ihre Mitarbeiter bestimmt. In der Verpflichtungserklärung werden die Mitarbeiter über die möglichen Verschwiegenheitspflichten und die Verpflichtung zur Wahrung von Betriebsgeheimnissen informiert.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Der Verantwortliche und die betreffenden Mitarbeiter |
| Wann muss ich dieses Dokument anlegen? | Sobald Ihr Unternehmen Mitarbeiter beschäftigt und diese in Berührung mit personenbezogen Daten kommen.  |
| Was ist sonst noch zu beachten? | Dieses Dokument sollte von allen Mitarbeitern unterschrieben werden |
| Dokumenttitel | Verpflichtungserklärung zur Wahrung von Datengeheimnissen.docxIT-Richtline Mitarbeiter.docxEvidenz Bewerberdaten.docx |

## Kategorie Grün – empfohlen!

###

### Data Breach-Protokoll und Notification

Eine Data Breach-Notification ist die Meldung einer Datenschutzverletzung bzw. eines dokumentierten Datenschutzmissbrauches.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Die Datenschutzbehörde bzw. Betroffene, wenn Sie eine Datenschutzverletzung melden. |
| Wann muss ich dieses Dokument anlegen? | Wenn personenbezogene Daten aus Ihrem Unternehmen gestohlen werden.  |
| Was ist sonst noch zu beachten? | Bitte prüfen Sie vor einer Meldung an die Behörde oder Betroffene, ob ein Data Breach wirklich vorliegt. z.B. beim Diebstahl eines Smartphones kann es reichen, wenn das Gerät über eine Zugriffskontrolle (Passwort verfügt) und ein Dritter nicht einfach so auf die Daten darauf zugreifen kann.  |
| Dokumenttitel | Data Breach Protokoll.docxData Breach Notification Behörde.docx |

### Muster Erteilung einer Auskunft

Im Dokument „Erteilung einer Auskunft“ wird eine mögliche Antwort auf einen Auskunftsbegehren von einem Betroffenen dokumentiert.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Nur der Betroffene, der um Auskunft ersucht.  |
| Wann muss ich dieses Dokument anlegen? | Nur wenn ein Betroffener Ihnen ein berechtigtes Auskunftsbegehren schickt.  |
| Was ist sonst noch zu beachten? | Achten Sie auf Ihre Prozesse der Betroffenenrechte  |
| Dokumenttitel | Musterauskunft.docx  |

### IT-Dokumentation

In der IT-Dokumentation sollte der aktuelle IST-Zustand ihrer IT-infrastruktur aufgezeichnet werden.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  | Nur der Verantwortliche und auf Verlangen die zuständige Datenschutzbehörde |
| Wann muss ich dieses Dokument anlegen? |  |
| Was ist sonst noch zu beachten? |  |
| Dokumenttitel | IT-Dokumentation.docx  |

### Schulungsunterlagen

Sammeln Sie alle Informationen zu Schulungen und Vorträgen zur DSGVO, die Sie oder Ihre Mitarbeiter besucht haben.

|  |  |
| --- | --- |
| Wer hat auf diese Dokument Zugriff?  |  |
| Wann muss ich dieses Dokument anlegen? |  |
| Was ist sonst noch zu beachten? |  |
| Dokumenttitel |  |