Datenschutz Grundverordnung DSGVO

Das Wichtigste für Gründer/innen knapp zusammengefasst

Aktualisiert: 13.6.2018
Zusammengestellt von: Christian Toller, tethis IT e.U., Wien
Auch online verfügbar: www.tethis-it.at/dsgvo-zusammenfassung
Die Vollständigkeit und Korrektheit dieses Dokumentes wird nicht garantiert.

Die Gesetze

Bisher: Datenschutzgesetz (DSG) 2000
Ab 25.5.2018:

- EU Datenschutzgrundverordnung (DSGVO)
- Österreichische Anpassungen: DSG 2018

Außerdem: E-Commerce Gesetz, Gewerbeordnung 1994, TKG

DSGVO in Kraft seit 24.5.2016, **verpflichtend ab 25.5.2018**

Aktuelle Änderungen

Am 14. April wurde die „Datenschutz Deregulierung 2018“ beschlossen:

- Angemessene Bestrafungen (Verhältnismäßigkeit)
- Beim ersten Verstoß wird nur verwarnt
- Günstigere Regelung (alt / neu) wird angewendet
- Behörden bleiben praktisch straffrei, keine Doppelbestrafung
- Keine Strafen für Spione
- Schadenersatzforderung durch Organisationen nicht möglich
- DSGVO gilt nicht für Journalisten
- Videoüberwachung zulässig

Siehe: https://www.wko.at/branchen/k/handel/versicherungsagenten/erleichterungen-bei-der-dsgvo.html

Strafen

2% / 10 Mio. €, in schweren Fällen 4% / 20 Mio. €
Datenschutzbehörde verhängt Strafen

Gültigkeitsbereich

Gilt für alle Firmen, die am EU Markt teilnehmen (also auch für ausländische Firmen)
Schützt personenbezogene Daten von lebender Personen sowie Firmen
Gilt NICHT für

- Daten aus der eigenen Familie und dem Freundeskreis
- Daten Verstorbener
- Anonymisierte Daten

Keine relevanten Ausnahmen für kleine Firmen!

Die Grundsätze des DSGVO

Die Verarbeitung (also Speicherung, Analyse, Verwendung) von personenbezogenen Daten ist prinzipiell verboten. Die Gesetze regeln nur die Ausnahmen.

1. Rechtmäßig und Transparent

Verarbeitung von personenbezogenen Daten nur erlaubt
- aus vertraglichen oder rechtlichen
- lebenswichtigen Interessen
- mit Erlaubnis des Betroffenen

Daten müssen rechtmäßig beschafft werden.
Betroffene Personen können Auskunft über die gespeicherten Daten verlangen.

2. Nur mit Zweckbindung

Bei der Zustimmung muss der Zweck der Datenspeicherung benannt werden.
Verarbeitung zu anderen Zwecken erfordert separate Zustimmung

3. So wenig wie möglich

Es dürfen nur so viele Daten erhoben und gespeichert werden, wie für den genannten Zweck notwendig sind.

4. Nur so lange wie nötig

Daten dürfen nur für eine bestimmte Dauer gespeichert werden.
Im Zweifel haben die gesetzlichen Aufbewahrungsfristen Vorrang.
Nach Ablauf dieser Frist müssen die Daten gelöscht werden.

5. Korrekt und sicher

Integrität und Vertraulichkeit
Die Daten müssen gegen versehentlichen Verlust oder Beschädigung geschützt werden
=> Datensicherung ist jetzt Pflicht
Die Daten müssen vertraulich bleiben
=> Zugangsschutz (Passwörter, Berechtigungen)
=> Verschlüsselung
=> Pseudonymisierung

Besonders schützenswerte Daten / sensible Daten

Machen eine Datenschutzfolgeabschätzung notwendig und erfordern konsequente Schutzmaßnahmen:

- Daten von Kindern (bis 14 Jahre)
- Rassische oder ethnische Herkunft
- Politische Meinungen
- Religiöse o. weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische oder biometrische Daten
- Gesundheitsdaten
- Sexualleben oder sexuelle Orientierung

Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung nicht-sensibler Daten:

Laut DSGVO	Grundlage
Art 6 Abs 1 lit a	Mit Einwilligung des Betroffenen
Art 6 Abs 1 lit b	Zur Erfüllung eines Vertrages
Art 6 Abs 1 lit c	Aufgrund rechtlicher Vorschriften
Art 6 Abs 1 lit d	Aus lebenswichtigen Interessen
Art 6 Abs 1 lit e	Bei öffentlichem Interesse
Art 6 Abs 1 lit f	Bei berechtigten Interessen des Verantwortlichen, sofern Rechte des Betroffenen nicht überwiegen (nicht bei Kindern)
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht

Rechtsgrundlagen für die Verarbeitung sensibler Daten:

Laut DSGVO	Grundlage
Art 9 Abs 2 lit a	Mit Einwilligung des Betroffenen
Art 9 Abs 2 lit b	Aufgrund Arbeits-/Sozialrecht, Kollektivvertrag, Betriebsvereinbarung
Art 9 Abs 2 lit c	Aus lebenswichtigen Interessen
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht
Art 9 Abs 2 lit f	Zur Geltendmachung von Rechtsansprüchen
Art 9 Abs 2 lit h	Für Zwecke der Gesundheitsvorsorge / Arbeitsmedizin
Art 9 Abs 2 lit g,l,j	Bei erheblichem öffentlichem Interesse (gesundheitlich, wissenschaftlich, historisch)

Rechte der betroffenen Personen

Recht auf Information (Datenschutzerklärung)

Der Betroffene muss, z.B. in einer Datenschutzerklärung, über folgende Punkte informiert werden:
- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Gesetzliche Grundlagen oder berechtigte Interessen
- Bei Weitergabe der Daten: Empfänger
- Werden Daten ins nicht-EU-Ausland transferiert? Wie wird die Anwendung der DSGVO sichergestellt?
- Dauer der Speicherung, Kriterien für Löschung
- Die Betroffenenrechte (diese Liste)
- Das Beschwerderecht
- Ob die Bereitstellung der Daten gesetzlich vorgeschrieben oder vertraglich notwendig ist und Folgen falls sie nicht bereitgestellt werden.
- Quelle der Daten (falls nicht direkt vom Betroffenen, z.B. Telefonbuch)

Recht auf Auskunft

Betroffene Personen haben das Recht auf Auskunft in klarer einfacher Sprache
Ergebnisse eigener Arbeit und geistiges Eigentum müssen nicht herausgegeben werden.
Alle Kontaktdaten, E-Mails, CRM Daten sind herauszugeben
Die Auskunft muss kostenlos sein, zumindest solange die Auskunftspflicht nicht missbraucht wird.

Recht auf Berichtigung, Löschung und Einschränkung

Der Betroffene hat das Recht die gespeicherten Daten zu korrigieren.
Er kann fordern, dass die Daten gelöscht werden. Ausnahme: Die Daten müssen aus gesetzlichen oder vertraglichen Gründen gespeichert werden.
Die Verwendung der Daten kann auf bestimmte Zwecke eingeschränkt werden.

Recht auf Datenübertragung

Der Betroffene kann die Übergabe von gespeicherten Daten an ein anderes Unternehmen fordern, z.B. an einen anderen Webhoster oder Mailprovider.

Recht auf Widerspruch

Ein einmal gegebenes Einverständnis zur Datenverarbeitung kann jederzeit widerrufen werden.

Für die Umsetzung dieser Rechte: 1 Monat, kann um 2 Monate verlängert werden.

Pflichten des Verantwortlichen

Der Verantwortliche, also derjenige der die Daten verarbeitet, hat folgende Pflichten

Informationspflicht & Umsetzung der Betroffenenrechte

Die Rechte der Betroffenen müssen umgesetzt werden.
Die Informationspflichten sind zu erfüllen (Datenschutzerklärung)

Umsetzung von Maßnahmen zum Datenschutz

Es sind, **in Hinsicht auf Risiko, Aufwand und Größe des Unternehmens angemessene,** technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen.

Privacy by Design

Eingesetzte Technologien sollten bereits mit Blick auf den Datenschutz entwickelt worden sein. Voreinstellungen sollte so gesetzt werden, dass sie dem Datenschutz gerecht werden.

Dokumentationspflicht

Die Datenverarbeitungsprozesse müssen in einem Verfahrensverzeichnis (siehe unten) dokumentiert werden.
Unternehmen unter 250 Mitarbeitern müssen das nur, wenn Daten nicht nur gelegentlich verarbeitet werden, sensible Daten verarbeitet werden oder ein Risiko für Rechte und Freiheiten besteht. In der Praxis: Jeder ist verpflichtet.

Außerdem muss nachgewiesen werden:

- Verpflichtung der Mitarbeiter auf Einhaltung des Datenschutzes
- Schriftliche Vereinbarungen mit Auftragsverarbeitern (siehe unten)
- Regelmäßige Überprüfungen der Maßnahmen & Dokumentation

Risikoanalyse

Das Risiko einer Datenschutzverletzung muss analysiert und gewichtet werden.
Sollte sich ein hohes Risiko ergeben, muss eine Datenschutzfolgeabschätzung durchgeführt werden. Anm.: Für „normale“ Anwendungen eher nicht nötig.

Meldung von Datenschutzverletzungen

Sollte eine Datenschutzverletzung auftreten, ist dies innerhalb von 72 Stunden der Aufsichtsbehörde zu melden, sofern ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
Sollte ein hohes Risiko bestehen, ist auch die betroffene Person zu informieren.
Eine Datenschutzverletzung wäre z.B. ein Hackerangriff, der Verlust eines Datenträgers, der Diebstahl eines Handys oder Laptops.

Zusammenarbeit mit der Datenschutzbehörde

Ernennung eines Datenschutzbeauftragten

Nur für Firmen, die sich primär mit der Verarbeitung von sensiblen Daten oder der Überwachung beschäftigen.
Für kleinere Firmen eher nicht relevant.

Auftragsverarbeitung

Wenn personenbezogene Daten an eine andere Firma zur Verarbeitung weitergegeben werden, so sind diese Firmen „Auftragsverarbeiter“.

Auftragsverarbeiter: Mailchimp, Microsoft Office 365, Webhoster, Cloud Datensicherung

Verantwortlicher (also nicht AV): Banken, Steuerberater, Versanddienstleister

Der Verantwortliche muss sich von Auftragsverarbeiter schriftlich zusichern lassen, dass dieser die DSGVO einhält.
Ein Vertrag mit einem Auftragsverarbeiter muss folgende Punkte enthalten:

- Bindung an den Verantwortlichen
- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der verarbeiteten Daten
- Kategorien der betroffenen Personen (sensible Daten?)
- Rechte und Pflichten des Verantwortlichen

Datenverarbeitung im Ausland

Datenverarbeitung innerhalb der EU unproblematisch

Außerhalb der EU nur…

- Wenn ein „Angemessenheits-Beschluss“ der EU Kommission vorliegt
  z.B. USA Privacy Shield, Kanada, Schweiz
- Wenn geeignete Garantien vorliegen (ISO Zertifizierung)
- Wenn ein Grund für eine Ausnahme vorliegt:
  - Ausdrückliche Einwilligung
  - Erfüllung eines Vertrages
  - Geltendmachung von Rechtsansprüchen
  - Lebenswichtige Interessen des Betroffenen
  - Öffentliches Interesse

Vorgehensweise bei der Umsetzung

1. ## Verfahrensverzeichnis mit folgenden Informationen erstellen
   Die DSGVO macht keine Vorschriften in Hinsicht auf den nötigen Detail-Level, also grob bleiben. D.h. „Buchhaltung“, „Marketing“, „Verkauf über Webshop“ wäre je ein Verfahren.
   - Name des Verantwortlichen
   - Name der Verarbeitung
   - Zweck der Verarbeitung
   - Kategorien der verarbeiteten Daten
   - Kategorien der betroffenen Personen
   - Kategorien der Empfänger
   - Übermittlung an Drittländer?
   - Fristen für Löschung (wenn möglich)
   - Allg. Beschreibung der TOMs (wenn möglich)
   - Rechtsgrundlage (ratsam, aber nicht von der DSGVO gefordert)
   - Auftragsverarbeiter (ratsam, aber nicht von der DSGVO gefordert)

2. ## Technische & organisatorische Maßnahmen (TOMs) auflisten.
   Das sind alle Maßnahmen, die dem Schutz der Daten dienen, z.B.
   - Passwortschutz
   - Zugangsbeschränkung (Berechtigungen)
   - Datensicherung
   - Verschlüsselung von Laptop und Handy
   - Virenschutz
   - Regelmäßige Updates
   - Weisungen für die Mitarbeiter (z.B. Vertrag, Datenschutzhandbuch)

3. ## Dringenden Verbesserungsbedarf identifizieren und umsetzen, z.B.
   - Virenscanner installieren
   - Datensicherung einrichten
   - Newsletteranmeldung mit Double-Opt-In einrichten

4. ## Risikoabschätzung, evtl. Datenschutzfolgeabschätzung
   - WKO Liste mit Kriterien prüfen und dokumentieren
   - Vorlage benutzen
   - Falls nötig Datenschutzfolgeabschätzung durchführen
   - Entscheiden, ob Datenschutzbeauftragter nötig ist
   - Entscheidungen dokumentieren

5. Datenschutzerklärung mit folgenden Punkten erstellen

- Verantwortlicher
- Welche Daten & Zweck der Verarbeitung
- Quelle, falls nicht selbst eingegeben
- Rechtsgrundlage
- Werden berechtigte Interessen verfolgt? Welche?
- Weitergabe an Drittstaaten? Ist der Empfänger "sicher"?
- Dauer der Speicherung, Kriterien für Löschung
- Werden automatisch Entscheidungen getroffen? Welche?
- Rechte des Betroffenen (Auskunft, Widerspruch, Beschwerde, etc.)
- Datenschutzbeauftragter, Kontaktdaten

6. Webseite: Sind Opt-Out oder Einwilligung nötig

Berechtigtes Interesse des Betreibers => Info und/oder Opt-Out
Interesse des Besuchers überwiegt => Einwilligung

Cookies => Info
Tracking => Info und Opt-Out (Google Analytics, Facebook Pixel)
JetPack, Akismet (Antispam) und ähnliches => Einwilligung, Finger weg!

Opt-Out wird z.B. mit Plugins realisiert (suche nach „Schweizer")

7. Einwilligungserklärungen formulieren

Eine korrekte Einwilligungserklärung muss:

- keiner bestimmten Form folgen
- dokumentierbar sein (also eher schriftlich, elektronisch)
- Freiwillig erfolgen (keine Abhängigkeiten)
- Für einen bestimmten Fall erfolgen (Zweck nennen)
- In informierter Weise erfolgen (nicht verstecken, klare Sprache)

Vorausgefüllte Erklärungen (gesetzter Haken) sind nicht zulässig.
„Kopplungsverbot" beachten!

8. Auftragsverarbeiter-Verträge einsammeln

- Newsletterversender, Webhoster, Anbieter von Clouddiensten anschreiben und Auftragsverarbeiter-Vertrag anfordern

9. Weisungen an Mitarbeiter dokumentieren

- Mitarbeiter müssen vertraglich zur Einhaltung des Datenschutzes verpflichtet werden

10. Regelmäßige Prüfung / Verbesserung

- Ist das Verarbeitungsverzeichnis vollständig?
- Haben sich die Risiken verändert?
- Wurden die TOMs umgesetzt?
- Sind die TOMs noch angemessen?
- Die jährliche Prüfung ist zu dokumentieren

Wichtige Links, Beispiele, Vorlagen

Österreichische Datenschutzbehörde (Gesetzestexte, Formulare, Leitfaden zur Umsetzung)
https://www.dsb.gv.at

WKO (Gesetze, Vorlagen, Checklisten):
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

WKO Checkliste zur Risikoabschätzung und Anleitung Datenschutzfolgeabschätzung:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

WKO Vorlage für eine Mitarbeitervereinbarung:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html

WKO IT-Safe: Tipps zu Datenschutzmaßnahmen, auch speziell für EPUs
https://www.wko.at/site/it-safe/start.html

WKO IT-Safe Fragebogen: Identifiziert Lücken im Datenschutz
https://itsafe.wkoratgeber.at/

WKO: Auswirkungen der DSGVO auf Webseiten und Webshops:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Auswirkungen-auf-Websites.html
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/datenverarbeitung-webshop-website.html

WKO: Bedingungen für erlaubten E-Mail-Versand:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/E-Mails_versenden_-_aber_richtig.html

RTR: Liste mit E-Mailadressen an die keine Werbung geschickt werden darf
https://www.rtr.at/de/tk/TKKS_ECGListe

WKO: Informationspflichten in einem Newsletter

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationspflichten_nach_dem_Mediengesetz_fuer_E-Mail-Ne.html

PrivacyOfficers.at, Verein österreichischer Datenschutzbeauftragter:
https://www.privacyofficers.at
z.B. Checkliste für die Umsetzung der DSGVO (eher für größere Unternehmen)
https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v1.0_24052017_FINAL.pdf

Stefan Hansen-Oest: Deutscher Anwalt mit pragmatischen Ansätzen zur DSGVO Umsetzung
http://www.datenschutz-guru.de

Stefan Hansen-Oest: Liste von möglichen TOMs zum Ankreuzen:
http://www.datenschutz-guru.de/files/Ausfuellhilfe_TOM_9_BDSG_V2.docx

Deutsche Hinweise zum Verarbeitungsverzeichnis mit vielen Beispielen:
https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Verzeichnis_der_Verarbeitungstaetigkeiten/Hinweise_zum_Verzeichnis_von_Verarbeitungstaetigkeiten.pdf

Privacy Shield, Liste der teilnehmenden US Unternehmen:
https://www.privacyshield.gov/participant_search

tethis IT: Beispiel einer Datenschutzerklärung inkl. Google Analytics, Mailchimp und Cloud-Diensten
https://tethis-it.at/dsgvo-informationspflichten/