

Datenschutz NEU

Wer ist betroffen? Was ist jetzt zu tun?

Mag. Florian Brutter
Oktober 2017



Wirtschaft sind wir alle.



Schutz des Menschen



Wirtschaft sind wir alle.



Grundlagen

➤ „Personenbezogene Daten“ (normale Daten)

- Grundsätzlich alle Informationen, die sich auf eine natürliche Person beziehen („betroffene Person“)
- Merke: Im Zweifel ist immer von personenbezogenen Daten auszugehen, z.B. Name, Geburtsdatum, Wohnadresse, Größe, Gewicht, Ausbildung, Einkommen- und Vermögensverhältnisse, Telefonnummer, Passnummer, Sozialversicherungsnummer, Familienstand, Vorlieben, Hobbys, Urlaubsort etc.

➤ „Sensible Daten“ (besonders geschützte Daten)

- Rassistische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, genetische Daten, biometrische Daten, Daten zum Sexualleben oder der sexuellen Orientierung

Wirtschaft sind wir alle.



Grundlagen

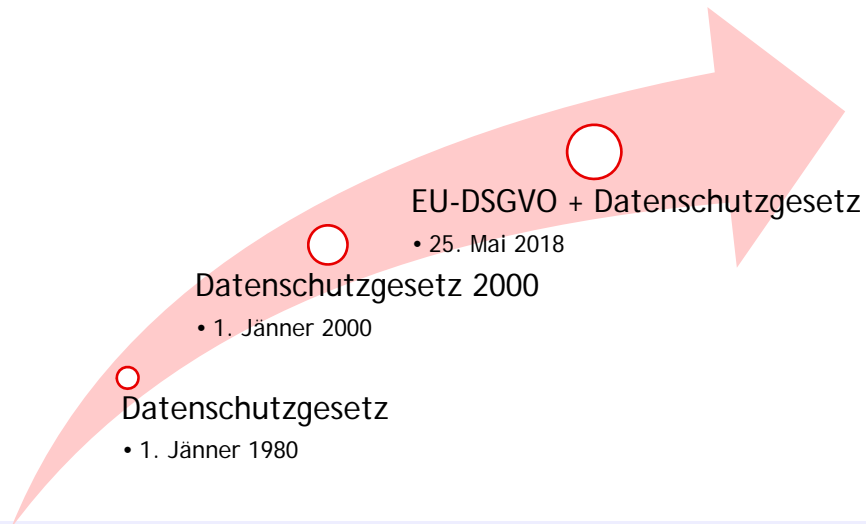
➤ „Verantwortlicher“

- Die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- Merke: Verantwortlicher ist immer der Rechtsträger des Unternehmens (z.B. GmbH) und nicht einzelne Organisationseinheiten oder Mitarbeiter im Unternehmen

Wirtschaft sind wir alle.



Österreich



Wirtschaft sind wir alle.



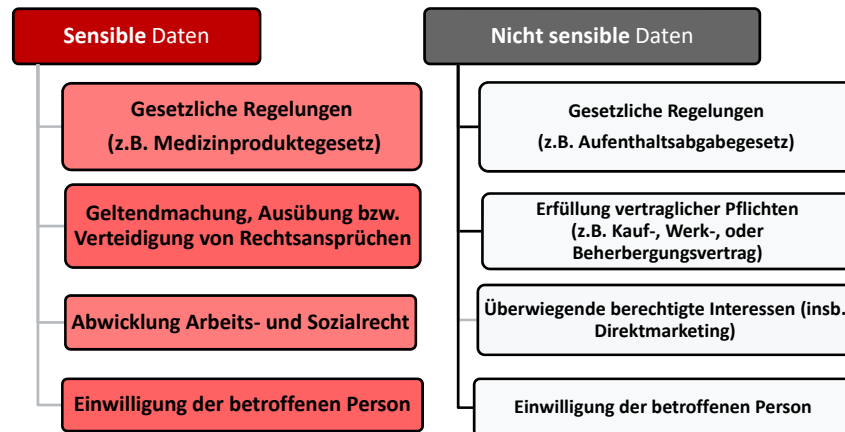
Datenschutzgrundverordnung - DSGVO

1. Keine Datenverarbeitung ohne Rechtsgrundlage
2. Anpassung von Einwilligungserklärungen
3. Verzeichnis über alle Verarbeitungstätigkeiten
4. Geeignete technische und organisatorische Maßnahmen (TOMs)
5. Datensicherheitsmaßnahmen
6. Datenschutz-Folgenabschätzung
7. Bestellung eines Datenschutzbeauftragten
8. Meldung von Datenschutz-Vorfällen
9. Informierung der Betroffenen
10. Ausreichende Transparenz
11. Datenübermittlung ins Ausland
12. Interne Datenschutzstrategien

Wirtschaft sind wir alle.



1. Rechtsgrundlagen



Wirtschaft sind wir alle.



2. Anpassung der Einwilligungserklärungen

- Nachweis der Einwilligung durch den Verantwortlichen
- Freiwilligkeit der Erklärung
 - Liegt nicht vor, wenn die Einwilligung eine zwingende Voraussetzung für die Leistungserbringung ist (z.B. Verhaltensanalyse bei gratis Internetdienst)
- Enthält die Einwilligung mehrere Sachverhalte (insb. Verwendungszwecke), muss diese in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen (besonders bei Kindern), dass die einzelnen Sachverhalte klar voneinander unterschieden werden können
- Jederzeitige Möglichkeit des Widerrufs - gilt pro futuro (ab Einlangen)
 - Pflicht des Verantwortlichen, auf Widerrufsrecht hinzuweisen
 - Widerruf muss so einfach wie möglich sein, wie die Erteilung
 - Erfolgt die Zustimmung z.B. über ein Webportal, muss daher auch der Widerruf über das Webportal erfolgen können (nicht per Einschreiben)

Altbestand: Bereits erteilte Zustimmungen nach dem DSG 2000 müssen auch den Anforderungen der DSGVO entsprechen, um aufrecht zu bleiben (§ 69 Abs. 9 DSG)

Wirtschaft sind wir alle.



3. Verzeichnis der Verarbeitungstätigkeiten

- Der Verantwortliche hat ein Verzeichnis über alle - in seiner Zuständigkeit liegenden - Verarbeitungstätigkeiten zu führen, das folgende Angaben enthält:
 - a) Namen und **Kontakt**daten des Unternehmens, des Vertreters des Verantwortlichen sowie eines allfälligen Datenschutzbeauftragten
 - b) Die **Zwecke** der Verarbeitung
 - c) Eine Beschreibung der **Kategorien** betroffener Personen und der Kategorien personenbezogener Daten
 - d) Die Kategorien von **Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern (z.B. Auftraggeber oder Kunden) oder internationalen Organisationen
 - e) **Übermittlungen** von personenbezogenen Daten an ein **Drittland** (gesonderte Auflistung der Länder) oder an eine internationale Organisation im Drittland
 - f) Wenn möglich, die vorgesehenen Fristen für die **Löschung** der verschiedenen Datenkategorien
 - g) Wenn möglich, eine allgemeine Beschreibung der getroffenen **Sicherheitsmaßnahmen**

Wirtschaft sind wir alle.



3. Verzeichnis der Verarbeitungstätigkeiten

- Die DSGVO befreit Unternehmen mit weniger als 250 Mitarbeitern von dieser Pflicht, allerdings nur dann, wenn
 - die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt (nicht also z.B. bei Videoüberwachung oder Kreditscoring)
 - keine sensiblen oder strafrelevanten Daten verarbeitet werden
 - die Datenverarbeitung **nur gelegentlich** erfolgt (was z.B. bei Buchungs- und Auftrags- oder Geschäftskundenverwaltung i.d.R. nicht der Fall sein wird)
- Merke: Die DSGVO sieht keine Regelungen zu Struktur und Form des Verzeichnisses vor
- **Empfehlung:**
 - Verwendung der Muster der Wirtschaftskammer (<https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html>) und
 - Orientierung an registrierte Meldungen in DVR-Online (<https://dvr.dsb.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx>)

Wirtschaft sind wir alle.



4. Geeignete technische und organisatorische Maßnahmen (TOMs)

- **Merke:** Im ersten Schritt ist zu prüfen, ob die Datenverarbeitung rechtmäßig ist (siehe zuvor die Rechtsgrundlagen). Im zweiten Schritt ist die Rechtmäßigkeit durch entsprechende Maßnahmen abzusichern
- **Merke:** Bei der Auswahl der Maßnahmen ist zumindest eine qualitative Risikobewertung vorzunehmen, die die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen berücksichtigt und zu einer der beiden Risikoklassen „normal“ oder „hoch“ führt
 - Bei der Verarbeitung von **sensiblen** Daten oder von Daten, deren Verarbeitung für die Betroffenen **bedeutende Auswirkungen** haben können, ist generell die Risikoklasse „hoch“ zu unterstellen, wenn eine Vielzahl von Personen betroffen ist und auch mehrere Mitarbeiter des Unternehmens an der Datenverarbeitung beteiligt sind
 - z.B. Verarbeitung von Gesundheitsdaten, Kreditscoring und Überprüfungen/Zertifizierungen)

Merke: TOMs sind regelmäßig zu evaluieren und gegebenenfalls anzupassen (**Audit**)

Wirtschaft sind wir alle.



4. Geeignete technische und organisatorische Maßnahmen (TOMs)

- Beispiele für **organisatorische** Maßnahmen sind:
 - Festlegung **interner Zuständigkeiten** und Verantwortlichkeiten (Rechteverwaltung)
 - Festlegung von **transparenten Verfahren** für die Bearbeitung von Anträgen, Anfragen und Beschwerden i. Z. m. Betroffenenrechten
 - Regelungen zur Speicherdauer/Löschung, Festlegung von Kriterien zur schnellstmöglichen Umstellung auf **Pseudonymisierung**, Verschlüsselung oder Anonymisierung
 - **Mitarbeiterschulungen** im Bereich Datenschutz
 - Festlegung verbindlicher Vorgehensweisen bei **Sicherheitsverletzungen**
 - Einführung und Überwachung von standardisierten **Prüf- und Kontrollverfahren**, die gewährleisten, dass Maßnahmen nicht nur am Papier stehen, sondern in der Praxis angewandt werden und funktionieren (Compliance System)

Wirtschaft sind wir alle.



4. Geeignete technische und organisatorische Maßnahmen (TOMs)

- Beispiele für **technische** Maßnahmen sind:
 - **Minimierung** der Datenverarbeitung
 - **Pseudonymisierung**
 - **Datenschutzfreundliche Voreinstellungen**
 - Durch Voreinstellung ist sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, die zur Erfüllung des jeweiligen Verarbeitungszwecks erforderlich sind, und zwar in Bezug auf
 - die Menge der erhobenen personenbezogenen Daten,
 - den Umfang der Verarbeitung dieser Daten,
 - die Speicherfrist dieser Daten und
 - die Zugänglichkeit dieser Daten
 - Keine automatische Voreinstellung von Einwilligungen

Wirtschaft sind wir alle.



5. Datensicherheitsmaßnahmen

- **Merke:** Die Pflicht zur Gewährleistung der Sicherheit von rechtmäßig verarbeiteten Daten entspricht dem aktuellen § 14 DSGVO 2018
- **Schutzziele** sind
 - die **Vertraulichkeit** der Daten (Schutz vor unbefugter Offenlegung und unbefugtem Zugang)
 - die **Integrität** der Daten (Schutz vor Veränderung)
 - die **Verfügbarkeit** der Daten (Schutz vor Vernichtung und Verlust)
- Beispiele für **Sicherheitsmaßnahmen** sind:
 - **Technische** Maßnahmen (Firewall, Anti-Malware Software, Systeme zur Datenwiederherstellung)
 - **Organisatorische** Maßnahmen (z.B. Mitarbeiterschulung, Verpflichtung zum Datengeheimnis)
 - **Physische** Sicherheitsmaßnahmen (z.B. Versperren von Türen, Verschlüsselung von Laptop-Festplatten)

Wirtschaft sind wir alle.



6. Datenschutz-Folgenabschätzung

- Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat das Unternehmen vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen
- **Empfehlung:** Aus Absicherungsgründen sollte eine Folgenabschätzung für alle Datenverarbeitungen durchgeführt werden, die in der Risikoklasse „hoch“ eingestuft sind
- Eine Folgenabschätzung hat zumindest folgende Inhalte aufzuweisen:
 - a) Eine systematische **Beschreibung** der Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten **berechtigten Interessen**
 - b) Die **Bewertung** der Notwendigkeit und **Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck
 - c) Die **Bewertung** der Risiken für die Rechte der Betroffenen (Identifikation potentieller Bedrohungsszenarien und Konfliktpotentiale)
 - d) Die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich **Garantien**, Sicherheitsvorkehrungen und Verfahren

Wirtschaft sind wir alle.



7. Bestellung eines Datenschutzbeauftragten

- Ein Datenschutzbeauftragter **muss** insb. dann benannt werden, wenn die **Kerntätigkeit** des Unternehmens in der umfangreichen Verarbeitung sensibler Daten oder in der systematischen Überwachung von Betroffenen besteht. In allen anderen Fällen **kann** ein Datenschutzbeauftragter freiwillig benannt werden
 - Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern dieser von jeder Niederlassung aus leicht erreicht werden kann (keine physische Erreichbarkeit erforderlich)
- Aufgaben** des Datenschutzbeauftragten:
- **Unterrichtung und Beratung** der Unternehmensleitung und der Mitarbeiter in allen datenschutzrechtlichen Angelegenheiten (inbs. Pflichten nach der DSGVO)
 - **Überwachung** und Überprüfung der Einhaltung der DSGVO, der anderen Datenschutzvorschriften, wobei dies auch die Zuweisung von Zuständigkeiten sowie die Sensibilisierung und Schulung von Mitarbeitern umfasst
 - **Anlaufstelle** für die Datenschutzbehörde
- **Merke:** Die Funktion des Datenschutzbeauftragten kann auch an einen externen Dienstleister ausgelagert werden

Wirtschaft sind wir alle.



8. Meldung von Datenschutz-Vorfällen

- Ab 25.5.2018 sind alle Verletzungen des Schutzes personenbezogener Daten (z.B. Verlust eines Firmenlaptops im Rahmen einer Dienstreise) unverzüglich und möglichst **innen 72 Stunden**, nachdem die Verletzung bekannt wurde, der Datenschutzbehörde zu melden
 - Eine Ausnahme von der Meldepflicht besteht dann, wenn der Vorfall voraussichtlich zu keinem Risiko für die Betroffenen führt (z.B. weil ihre Daten pseudonymisiert oder verschlüsselt waren)
- Merke: Der Tatbestand der Meldepflicht ist noch nicht verwirklicht, wenn bloß eine Verletzung der jederzeitigen Verfügbarkeit von Daten (z.B. Serverausfall) vorliegt
- Merke: Über meldepflichtige Vorfälle sind auch die betroffenen Personen unverzüglich zu informieren, wenn voraussichtlich ein hohes Risiko für ihre persönlichen Rechte und Freiheiten vorliegt, wovon z.B. bei sensiblen Gesundheitsdaten auszugehen ist
 - Es gelten grundsätzlich dieselben Ausnahmen wie bei der Meldung an die Datenschutzbehörde

Wirtschaft sind wir alle.



9. Information der Betroffenen

Werden künftig Daten **bei** der betroffenen Person erhoben (insb. weil sie von dieser Person **selbst zur Verfügung gestellt werden**), ist diese zum **Zeitpunkt** der Erhebung dieser Daten darüber zu **informieren**

- z.B. Online-Anfrage, Buchungsanfrage

- Folgende Informationen sind mitzuteilen, wenn und soweit die betroffene Person darüber nicht schon verfügt:
 - a) Namen und Kontaktdaten des Unternehmens und gegebenenfalls des Datenschutzbeauftragten
 - b) Die **Verwendungszwecke** und die **Rechtsgrundlage** für die Verarbeitung
 - c) Wenn Rechtsgrundlage eine **Interessenabwägung** ist, die entsprechenden berechtigten Interessen
 - d) Gegebenenfalls die **Empfänger** oder Kategorien von Empfängern der personenbezogenen Daten
 - e) Gegebenenfalls die Absicht, die personenbezogenen Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln

Zusätzliche Informationen sind mitzuteilen, wenn diese im Interesse einer fairen und transparenten Verarbeitung notwendig sind (vgl. im Detail Artikel 13 DSGVO)

Wirtschaft sind wir alle.



9. Information der Betroffenen

- Werden personenbezogene Daten **nicht bei** der betroffenen Person erhoben, so hat das Unternehmen ihr folgendes mitzuteilen, wenn und soweit sie darüber nicht schon verfügt:
 - a) Namen und Kontaktdaten des Unternehmens und gegebenenfalls des Datenschutzbeauftragten
 - b) Die Verwendungszwecke und die Rechtsgrundlage für die Verarbeitung
 - c) Die Kategorien personenbezogener Daten, die verarbeitet werden
 - d) Gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
 - e) Gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln
- Zusätzliche Informationen sind mitzuteilen, wenn diese im Interesse einer fairen und transparenten Verarbeitung notwendig sind (vgl. im Detail Artikel 14 DSGVO)

Wirtschaft sind wir alle.



10. Ausreichende Transparenz

- Das Unternehmen hat geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen und Mitteilungen nach der DSGVO zu übermitteln, und zwar in
 - präziser, transparenter, verständlicher und leicht zugänglicher Form (z.B. in Form eines Links „Datenschutzerklärung“ auf der Webseite) und
 - einer klaren und einfachen Sprache, insb. wenn Kinder (bis 14 Jahre) von der Datenverarbeitung betroffen sind
- Neue Verfahrensfristen:
 - Sämtliche Mitteilungen/Maßnahmen im Rahmen der Umsetzung oder Erfüllung von Rechten der Betroffenen haben künftig unverzüglich (d.h. ohne schuldhafte Verzögerung), jedenfalls aber **innen 1 Monat** zu erfolgen. Diese Frist ist (abhängig von der Komplexität und Anzahl der Anträge) um 2 weitere Monate verlängerbar
 - Dies betrifft auch bereits bestehende Rechte (wie z.B. Recht auf Auskunft, Löschung oder Widerspruch)
 - Vereinheitlichung aller Verfahren zur Wahrung der Betroffenenrechte







Wirtschaft sind wir alle.



10. Ausreichende Transparenz

➤ Standardisierte Bildsymbole

- Informationen/Mitteilungen können in **Kombination** mit Bildsymbolen erfolgen („to be presented by the icons“)
- Die **Europäische Kommission** ist ermächtigt, solche Bildsymbole verpflichtend vorzusehen und das Verfahren dazu zu regeln. Bis dahin erfolgt die Darstellung mit Bildsymbolen **freiwillig**

SYMBOL	WESENTLICHE INFORMATIONEN	BEZUG
	Es werden nicht mehr personenbezogene Daten erhoben , als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Es werden nicht mehr personenbezogene Daten gespeichert , als für die spezifischen Zwecke der Verarbeitung erforderlich sind.	
	Personenbezogene Daten werden nicht zu anderen als den Zwecken verarbeitet , für die sie erhoben wurden.	
	Es werden keine personenbezogenen Daten an gewerbliche Dritte weitergegeben .	
	Es werden keine personenbezogenen Daten verkauft oder verpachtet .	
	Es werden keine personenbezogenen Daten unverschlüsselt aufbewahrt.	

Quelle: www.handelsblatt.com

Wirtschaft sind wir alle.



11. Datenübermittlung ins Ausland

- Der Datenverkehr **innerhalb** der EU/EWR unterliegt keinen besonderen Beschränkungen
- Der Datenverkehr **von Drittländern nach Österreich** liegt grds. im Verantwortungsbereich des Datenübersmittlers im Drittstaat (insb. nach dessen nationalen Rechtsvorschriften)
- Der Datenverkehr **von Österreich in Drittländer** ist nur nach Maßgabe der **Artikel 44 ff. DSGVO** zulässig, z.B. aufgrund
 - eines **Angemessenheitsbeschlusses** der Europäischen Kommission, z.B. USA (für Unternehmen, die sich der **Privacy-Shield** Vereinbarung unterworfen haben), Argentinien, Israel, Kanada, Neuseeland, Schweiz
 - von **Standarddatenschutzklauseln**, die von der Europäischen Kommission erlassen wurden
 - verbindlichen **internen Datenschutzvorschriften** (Binding corporate rules), die für eine gesamte Unternehmensgruppe bzw. eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, ausgearbeitet, der Datenschutzbehörde vorgelegt und von dieser abgesegnet wurden
 - der **ausdrücklichen Einwilligung** des Betroffenen (nach Unterrichtung über die Risiken einer Übermittlung ohne Vorliegen eines Angemessenheitsbeschlusses oder geeigneter Garantien)

Wirtschaft sind wir alle.



12. Interne Datenschutzstrategien

- Unternehmen haben im Wege von internen Datenschutzstrategien die Umsetzung der geeigneten technischen und organisatorischen Maßnahmen („TOMs“) nachzuweisen
- Aus Zweckmäßigkeitsgründen können in diesen internen Datenschutzstrategien insb. auch folgende Inhalte aufgenommen werden:
 - Das Verzeichnis der Verarbeitungstätigkeiten
 - Die Einhaltung der Grundsätze für die Datenverarbeitung (Artikel 5 DSGVO)
 - Beschreibung der getroffenen Datensicherheitsmaßnahmen
 - Dokumentation der Datenschutz-Folgenabschätzung
 - Dokumentation des Verfahrens zur Einhaltung der Melde- und Informationspflichten
 - Dokumentation der standardisierten Abläufe bei Datenübermittlungen ins Ausland

Wirtschaft sind wir alle.



Fahrplan bis 25. Mai 2018

1. Erstellung eines Verzeichnisses über alle Verarbeitungstätigkeiten (Bestandsaufnahme)
2. Durchführung einer Risikobewertung und Implementierung geeigneter „TOMs“
3. Prüfung und gegebenenfalls Adaptierung der Datensicherheitsmaßnahmen
4. Durchführung der Folgenabschätzung bei Datenverarbeitungen, die der Risikoklasse „hoch“ zugeordnet werden
5. Beschreibung einer zielführenden Auditierung
6. Verfahrensanleitungen zur
 - a) Einhaltung der Grundsätze für die Datenverarbeitung
 - b) Erfüllung von Informations- und Meldepflichten
 - c) Wahrung der Betroffenenrechte (Transparenz)
 - d) Prüfung von Datenübermittlungen ins Ausland
 - e) zeitlichen Vornahme der Pseudonymisierung
7. Zusammenfassung der Punkte 2 bis 6 in internen Datenschutzstrategien
8. Absicherung bei Outsourcing (Anpassung von Dienstleisterverträgen)

Wirtschaft sind wir alle.



Nützliche links

- **Informationsangebot der Wirtschaftskammern**
 - www.wko.at/datenschutz
- **Online-Ratgeber DSGVO**
 - dsgvo.wkoratgeber.at
- **Ratgeber zu den Informationspflichten DSGVO**
 - dsgvo-informationsverpflichtungen.wkoratgeber.at
- **Online-Ratgeber It-Safe**
 - it-safe.wkoratgeber.at
- **Österreichisches Informationssicherheitshandbuch**
 - www.sicherheitshandbuch.gv.at

Wirtschaft sind wir alle.

