EU-Datenschutz-Grundverordnung (DS-GVO)

19. Oktober 2017

Ihre Ansprechpartner

Mag. Wolfgang Rachbauer
Partner, Steuerberater
rachbauer@wtar.at

Sascha Bauer
sbcom GmbH

Inhalt

- Was ist die EU-Datenschutz-Grundverordnung (DS-GVO)?
- Welche Unternehmen sind betroffen?
- Rechte der Kunden
- Erweiterung für Personen / Unternehmen
- Was passiert bei Verstößen?
- Worauf kommt es an?
- Datenschutzbeauftragter
- Brennpunkte identifizieren
- Workflows und Tools überprüfen
- IT-Infrastruktur überprüfen und absichern
- Umsetzung in der Praxis
- Grundregel

Was ist die EU-Datenschutz-Grundverordnung (1)?

- Verabschiedung im April 2016 vom europäischen Parlament
- Regelt die europaweite Modernisierung und Vereinheitlichung von Datenschutzgesetzen
- Ziel: Garantieren des Schutzes von personenbezogenen Daten im Hinblick auf
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit

Was ist die EU-Datenschutz-Grundverordnung (2)?

Die Verordnung ersetzt die in die Jahre gekommene Data Protection Directive (DPD) von 1995. Anders als die DPD ist die DS-GVO nicht „nur“ eine Richtlinie, sondern **tatsächlich ein Gesetz**. Das bedeutet, dass die Verordnung nicht separat von den EU-Mitgliedsstaaten implementiert werden muss. **Das Datum des Inkrafttretens war deshalb schon der 24. Mai 2016.** Um Unternehmen die Zeit zu geben, sich an die neue Gesetzeslage anzupassen, wurde eine **Übergangsfrist bis zum 25. Mai 2018** eingeräumt. **Bis zu diesem Datum haben Unternehmen Zeit, die Vorgaben der DS-GVO umzusetzen.** Bleibt dies aus, können bei einer Datenschutzpanne hohe Strafen verhängt werden. In Österreich wird dies zusätzlich noch durch das Datenschutzgesetz aus dem Jahr 2000 geregelt. Begleitend (für kritische Infrastrukturen) tritt ab 9. Mai 2018 noch NISG 2018 in Kraft.

Welche Unternehmen sind betroffen (1)?

DS-GVO regelt den Schutz von personenbezogenen Daten

→ **Deshalb sind alle Unternehmen, die personenbezogene Daten von Privatpersonen in der europäischen Union verarbeiten, betroffen.**

Definition in Artikel 4 des Gesetzestexts:
„Im Sinne dieser Verordnung bezeichnet der Ausdruck personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“

Welche Unternehmen sind betroffen (2)?

Die Definition ist also sehr weit gefasst. **Typische Daten**, die von Unternehmen gesammelt und von der DS-GVO geschützt werden, sind **der Name, die Anschrift, die E-Mail-Adresse oder auch die IP-Adresse**. Im Unternehmenskontext geht es dann oft um Kundendaten, die zB. in einem CRM-System verarbeitet werden. Aber **auch Daten, die nur für Marketingzwecke verwendet** oder auch als „Beifang“ aufgezeichnet werden, wie zB. eine IP-Adresse in einer Log-Datei, werden von der DS-GVO geschützt.

Welche Rechte haben Kunden in der DS-GVO (1)?

Die DS-GVO beschreibt die Vorgaben, die Unternehmen umsetzen müssen, wenn sie personenbezogene Daten verarbeiten. Obwohl viele Maßnahmen schon in der Data Protection Directive definiert wurden, gibt es ein paar neue Anordnungen, die selbst für Unternehmen, die bis jetzt immer „compliant“ waren, eine Herausforderung darstellen werden. Ein kurzer Überblick:

- **Recht auf Vergessenwerden:** Kunden haben „das Recht, zu verlangen, dass ihre personenbezogenen Daten gelöscht werden“ (Artikel 17).
- **Zweckbindung und das Recht auf Zustimmung:** Teilweise ist diese bereits im DSG festgeschrieben, wird aber in der DS-GVO konkretisiert. Jeder Kunde muss „umfassend und in einfacher Sprache“ über den Verwendungszweck von Daten, die er preisgibt, informiert werden. Die Einwilligung zur Nutzung muss freiwillig erfolgen – sie darf also nicht an andere Bedingungen geknüpft sein (zB. das Einwilligen zur werblichen Verwendung der Daten, um eine Bestellung abschließen zu können); dies ist im Erwägungsgrund Nr. 42 sowie 43 zur DS-GVO festgeschrieben.

Welche Rechte haben Kunden in der DS-GVO (2)?

- **Zügige Meldung an die Aufsichtsbehörde:** „Im Fall einer Verletzung des Schutzes meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde“ (Artikel 33).
- **Recht auf Datenübertragbarkeit:** Kunden haben das Recht, die über sie gespeicherten Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“ (Artikel 20).

Welche Rechte haben Kunden in der DS-GVO (3)?

Klar ist, dass die **Umsetzung** dieser Rechte und deren Abbildung in Unternehmensprozessen **nicht trivial** sind. Zum Beispiel setzen viele Vorgaben voraus, dass Unternehmen wissen, in welchem Umfang und an welchen Stellen sie personenbezogene Daten gespeichert haben. Das kann in einer kleinen Firma mit nur einer zentralen Kundendatenbank noch zutreffen, aber spätestens beim Betrachten von Datenquellen wie Videoüberwachungen in öffentlich zugänglichen Räumen oder auch bei Verarbeitung von Daten in Cloud-Plattformen (wie zB. Salesforce) wird klar, dass viele Firmen viel mehr personenbezogene Daten speichern und verarbeiten, als ihnen vielleicht bewusst ist und diese auch außerhalb des eigenen direkten Einflussbereichs gespeichert oder verarbeitet werden. **Auch gibt es Konfliktpotenzial, wenn ein Kunde Daten löschen lassen möchte, diese aber im Rahmen von anderen Gesetzen aufbewahrt werden müssen (wie zB. Rechnungsdaten).**

Wesentliche Erweiterung für Personen

- Mehr Transparenz für die Betroffenen
- Betonung der Datenminimierung ➔Recht auf Vergessen
- Begrenzung der Speicherung
- Sensible Daten um biometrische und genetische Daten erweitert
- Informationspflichten erweitert über: Verantwortlicher, Vertreter, Datenschutzbeauftragter, Beschwerderechte, automatische Entscheidungen, Profiling, Übermittlungen
- Information des Betroffenen für Daten aus anderen Quellen
- Auskunftspflicht auf 1 Monat verkürzt (samt Negativauskunft)
- Einschränkung der Verarbeitung für bestimmte Daten
- Datenportabilität (keine Behinderung durch Verantwortlichen)
- Widerspruch zu automatischen Entscheidungen und Profiling (Hinweis darauf Pflicht, Vereinfachung beim Widerspruch)

Wesentliche Erweiterung für Unternehmen

- Mehr Sicherheit in der Verarbeitung mit Nachweispflicht
- Privacy by Design und by Default für IT-Produkte und Services (hat starke Auswirkungen im Zivil- und Unternehmensrecht)
- Auftragsverarbeiter (= Dienstleister) werden stärker in die Pflicht genommen
- Vertreter Benennung für Nicht-EU-Unternehmen
- Verarbeitungsverzeichnis statt Meldung in DVR, dadurch wesentlich mehr Sicherheit, wenn ernst genommen, sonst hohe Geldbußen
- Informationspflichten bei Verletzung des Datenschutzes binnen 72 Stunden an Aufsichtsbehörde und Betroffene
- Datenschutz-Folgenabschätzung bei neuen Technologien, hohen Risiken, (sonst hohe Geldbußen)
- Datenschutzbeauftragter für öffentliche Stellen und Behörden Pflicht, sonst Kannbestimmung; unabhängig, keine Weisungen, intern/extern möglich, Einbindung in alle IT- und Sicherheitsfragen
- Zertifizierungen erleichtern Beweispflichten, befreien aber nicht

Was passiert bei Verstößen gegen die DS-GVO (1)?

Nicht nur die in der DS-GVO beschriebenen Maßnahmen sind neu, auch die **Bußgelder** für Unternehmen, die diese entweder nicht oder nur mangelhaft umsetzen, **wurden neu definiert**. Wenn eine Datenschutzbehörde einen Verstoß feststellt, können – je nach Schwere eines Falls – folgende Bußgeldbeträge fällig werden:

- Bis zu € 20 Million oder 4 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)
- Bis zu € 10 Million oder 2 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)

Was passiert bei Verstößen gegen die DS-GVO (2)?

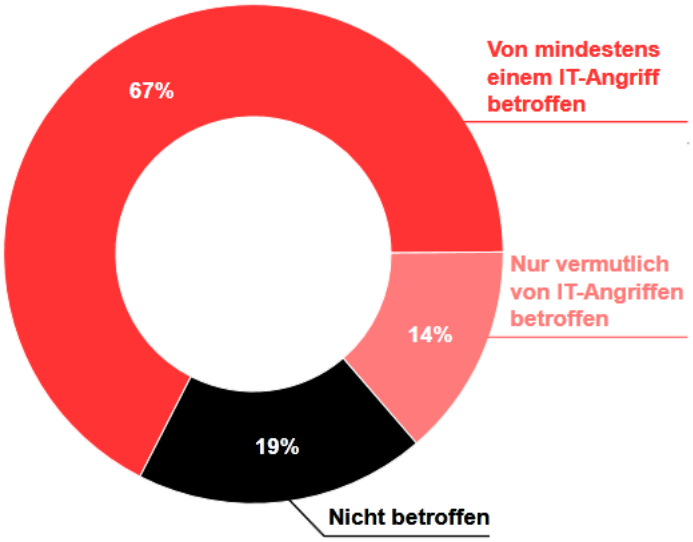
Die erste Bußgeldkategorie wird zum Beispiel angewendet, wenn ein Unternehmen gegen Bestimmungen im Artikel 17 (Recht auf Vergessenwerden) verstößt. Letztere Kategorie ist für verhältnismäßig kleine Verstöße gedacht, wie zB. eine Verletzung der Meldepflicht nach Artikel 33, kann jedoch bei einem Maximalbetrag von € 10 Million oder 2 % des Umsatzes immer noch sehr hoch ausfallen. Die Bußgelder werden im Artikel 83 der DS-GVO definiert, der des Weiteren sicherstellt, dass die Verhängung von Geldbußen in jedem Fall „wirksam, verhältnismäßig und abschreckend“ ist. Für Österreich hat sich seit dem Inkrafttreten der DS-GVO auch die Haftung geändert: In den Artikel 41 bis 43 des Datenschutz-Anpassungs- und –Umsetzungsgesetzes (DSAnpUG) sind **auch Sanktionsmöglichkeiten gegen natürliche Personen vorgesehen**, nicht nur gegen Unternehmen. **Sprich: Auch ein Datenschutzbeauftragter oder ein Geschäftsführer kann für Verstöße persönlich haftbar gemacht und ggf. in Regress genommen werden.**

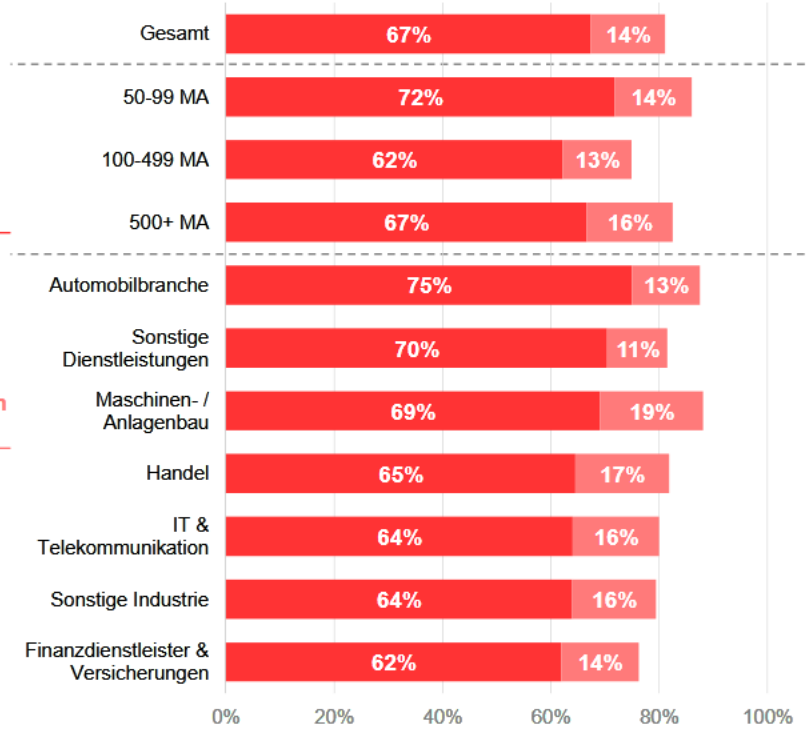
Der Countdown läuft – Worauf kommt es an?

Trotz möglicher hoher Geldstrafen und der schnell ablaufenden Übergangsfrist **haben viele Firmen noch keine Vorkehrungen getroffen**. Laut Gartner wird bis Ende 2018, wenn die Verordnung schon längst in Kraft getreten ist, immer noch mehr als die Hälfte der von der DS-GVO betroffenen Unternehmen nicht alle Vorgaben umgesetzt haben. Mit so vielen möglichen Auswirkungen ist es wichtig, einen Überblick über die Implementierungsschwerpunkte zu bekommen.

Zwei Drittel der Unternehmen sind von IT-Vorfällen betroffen

Großteil der Unternehmen hat IT-Sicherheitsvorfälle festgestellt oder zumindest vermutet. Finanzdienstleister und Versicherungen sind vergleichsweise seltener das Angriffsziel.





Frage: „War Ihr Unternehmen innerhalb der letzten 12 Monate von IT-Sicherheitsvorfälle betroffen bzw. vermutlich betroffen?" | Basis: Alle Unternehmen ab 50 Mitarbeiter (n=750)

bitkom research F-Secure.

Datenschutzbeauftragter (1)

Der erste Schritt ist die Benennung oder Bestellung eines Datenschutzbeauftragten (DSB). Dies **gilt gemäß Artikel 37 für Behörden, öffentliche Stellen und Unternehmen, die personenbezogene, sensible Daten verarbeiten**. Für kleine und mittelständische Firmen kann auch die Benennung eines externen Datenschutzbeauftragten in Betracht gezogen werden. Der Datenschutzbeauftragte muss sowohl gegenüber der Öffentlichkeit als auch der zuständigen Landesdaten-schutzbehörde als offizieller Ansprechpartner benannt werden. Aber auch Firmen, die nicht zur Benennung eines Datenschutzbeauftragten verpflichtet sind, können davon profitieren, zB. um eine Anlaufstelle für interne und externe Fragen bezüglich Datenschutz zu etablieren.

Datenschutzbeauftragter (2)

Die DS-GVO erlegt Unternehmen gemäß Art. 37 Abs.1 DS-GVO die Verpflichtung auf, einen betrieblichen Datenschutzbeauftragten zu benennen, wenn die Kerntätigkeit eines Verantwortlichen bzw. eines Auftragsverarbeiters in der Durchführung solcher Verarbeitungsvorgänge liegt, **die eine umfangreiche, regelmäßige und systematische Überwachung betroffener Personen erforderlich machen oder wenn die Verarbeitungsvorgänge die Verarbeitung sensibler Daten umfassen.**

Eine Öffnungsklausel in Art. 37 Abs. 4 DS-GVO ermöglicht es dem nationalen Gesetzgeber, die Bestellung eines Datenschutzbeauftragen auch in weiteren Fällen vorzuschreiben. Es ist wahrscheinlich, dass der österreichische Gesetzgeber von dieser Möglichkeit Gebrauch machen wird; ob dies auch für Sonderregelungen zum Status des Datenschutzbeauftragten der Fall sein wird und kann, ist mit Blick auf den begrenzten Regelungsgehalt der Öffnungsklausel hingegen keineswegs sicher.

Brennpunkte identifizieren

Für jede Firma, egal welcher Größe, können folgende Fragen dabei helfen, die Brennpunkte für die Umsetzung zu identifizieren:

- Welche von der DS-GVO betroffenen Daten werden im Unternehmen gesammelt oder verarbeitet?
- Werden die Daten ausreichend geschützt? Entspricht die eingesetzte Technologie dem Stand der Technik?
- Kann im Fall einer Datenschutzverletzung innerhalb von 72 Stunden eine Meldung an die Datenschutzbehörde verschickt werden?
- Können Kunden Auskunft über die über sie gespeicherten Daten bekommen bzw. kann die Löschung der Daten durchgeführt werden?
- Werden Daten zur Speicherung oder Verarbeitung an andere Unternehmen übermittelt (zB. Cloud-Dienste)? Müssen hier gegebenenfalls Anpassungen in den Verträgen zur Auftrags-Datenverarbeitung vorgenommen werden? Wichtig hier: es gibt keinen „Bestandsschutz“ für Altverträge.

Workflows und Tools überprüfen

Dabei gilt es, sowohl die **Mitarbeiter für das Thema** zu **sensibilisieren** als auch die **Workflows und Tools** zu **überprüfen** und ggf. auf einen gesetzeskonformen Stand zu bringen. Die Erstellung von Compliance-Regeln, die den Umgang mit Informationen festlegen, ist hier ein wichtiger Schritt. Solche Regeln stellen eine Kombination aus technischen und organisatorischen Maßnahmen dar. So kann zB. auf der Technologieebene ein Policy Management dafür sorgen, dass nur die für die Datenverarbeitung notwendigen Tools verwendet werden können – und Anwendungen wie zB. private Cloud-Speicherdienste nicht. Auch die Benutzung von externen Geräten soll unterbunden werden, damit Mitarbeiter die personenbezogenen Daten nicht auf zB. USB-Sticks abspeichern können.

IT-Infrastruktur überprüfen und absichern

Ein weiterer wichtiger Baustein ist die **umfassende Absicherung der IT-Systeme**. Bestehende Systeme müssen überprüft und neue Systeme ggf. eingeplant und ausgerollt werden. Der **Schutz fängt schon auf** der **Netzwerk- und Kommunikationsebene an**. Um unerlaubte Verbindungen zu unterbinden, soll eine Firewall verwendet werden. Web-Verkehr und andere Kommunikationswege aus dem Internet sollten gründlich überprüft werden, zB. von einer Web-Schutz-Komponente oder auch einem E-Mail-Scan. Schutz gegen bösartige Malware kann mit Hilfe einer proaktiven Dateisystem- und Prozessüberwachung sichergestellt werden. Um dafür zu sorgen, dass das Betriebssystem und die Anwendungen auf dem aktuellsten Stand sind und Schwachstellen rechtzeitig behoben werden, kann ein Patch-Management-System dabei helfen, den Überblick über die Patchverteilung zu behalten. **Nicht zuletzt ist die Datensicherung sehr relevant**: **Um dafür zu sorgen, dass Daten nicht verloren gehen können, muss ein Backup- und Wiederherstellungskonzept erarbeitet werden.**

Umsetzung in der Praxis – DS-GVO (1)

Da IT-Prozesse nicht nur technische, sondern auch organisatorische Funktionen beinhalten, dauert es in der Praxis relativ lange, bis sie wirksam werden.

Daher muss man **früh planen und vorbereiten**:

1. Information der Geschäftsleitung (da IT-Prozesse und Organisation involviert)
2. Identifizierung aller Prozesse mit und ohne personenbezogenen Daten, aber mit Querverbindungen dazwischen **(Verarbeitungsverzeichnis)**
3. Zweckbestimmung und Rechtsgrundlagen dazu (Zustimmungen, Vertrag, Gesetz, Bescheide, Urteile)
4. Risikobestimmung für jeden Prozess (Datenverlust: vorsätzlich / fahrlässig / zufällig; Löschung; Verändern; Kopieren; Übermittlungen)
5. Folgeabschätzungen für jeden Prozess
6. Informations- / Dokumentationslücken feststellen und schließen

Umsetzung in der Praxis – DS-GVO (2)

7. Auftragsverarbeiter (Verträge, Meldepflichten, Haftungen, Kontrollen, Probleme usw.)
8. Löschungskonzepte (aktuelle Datenbanken, Backup)
9. Sicherheitskonzepte verbessern und umsetzen
10. Prozessanpassungen (Identifikation, Auswirkungen, Dauer, Verantwortung, Kosten)
11. Protokolle Logdateien (Sicherung, Dauer, digitale Signaturen, Zugriff, Backup)
12. Betriebsvereinbarungen
13. Informationspflichten Aufsichtsbehörde, Betroffene
14. Mitarbeiterschulungen

Grundregel

- Die Verwendung personenbezogener Daten grundsätzlich vermeiden oder auf das absolut notwendige Maß beschränken!
- Sie sollten sich immer fragen: “Wer braucht sie, warum, wozu, wie lange und ist das auch rechtlich gedeckt (freie Zustimmung / gültiger Vertrag / Gesetz / rechtskräftiger Bescheid oder Urteil)?

Goldene Regel

„Was du nicht willst, dass man dir tu‘, das füg auch keinem andern zu!“

Die Goldene Regel als ethischer Grundsatz ist über 3000 Jahre alt und von China (Konfuzius, 551 – 479 v. Chr.) bis Spanien (Isidor von Sevilla, 560 – 636 n. Chr.) als Grundprinzip des richtigen Handelns gefordert. Sie gehört zu den fundamentalen Rechtsgrundsätzen.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Bitte beachten Sie, dass dieser Vortrag als Denkanstoß zu den möglichen Auswirkungen der DS-GVO gedacht ist und eine umfassende rechtliche Beratung nicht ersetzt.

Scharfe Analyse und feuriger Einsatz

ergeben Beratung mit der richtigen Würze!

ASCHAUER & RACHBAUER OG Steuerberatungsgesellschaft
Hochstraße 1 | 4060 Leonding | Tel. 0732/672492