Die wichtigsten Fragen und Antworten auf einen Blick

FAQ Datenschutz-Grundverordnung (DSGV, englisch: General Data Protection Regulation, GDPR)

Q: Wie wirkt sich die Datenschutz-Grundverordnung auf Unternehmen aus?
A: Die Datenschutz-Grundverordnung enthält viele Anforderungen über die Art der Erfassung, Aufbewahrung und Nutzung persönlicher Informationen. Dies beinhaltet nicht nur, wie persönliche Daten in den Systemen erkannt und geschützt werden, sondern auch wie neue Transparenzanforderungen eingebunden, Verstöße gegen persönliche Daten erkannt und gemeldet sowie Datenschutzpersonal und -mitarbeiter geschult werden.
Angesichts der enormen Bedeutung sollten Unternehmen mit den Vorbereitungen nicht warten, bis die Verordnung am 25. Mai 2018 in Kraft tritt, sondern jetzt mit der Prüfung der Vorgehensweisen beim Datenschutz und bei der Datenverwaltung beginnen. Verstöße gegen die Datenschutz-Grundverordnung werden mit erheblichen Bußgeldern und Reputationsschäden bestraft.

Q: Welche Rechte müssen Unternehmen unter der Datenschutz-Grundverordnung gewähren?
A: Die Datenschutz-Grundverordnung gewährleistet in der EU ansässigen Personen durch einen Katalog von Betroffenenrechten die Kontrolle über ihre personenbezogenen Daten. Dies schließt die folgenden Rechte ein:

- Zugriff auf leicht zugängliche und klare sowie verständliche Informationen über die Art der Nutzung personenbezogener Daten
- Zugriff auf personenbezogene Daten
- Löschung oder Korrektur fehlerhafter personenbezogener Daten
- unter bestimmten Umständen Richtigstellung und Löschung personenbezogener Daten (so genanntes „Recht auf Vergessenwerden“)
- Einschränkung der und Widerspruch gegen Verarbeitung personenbezogener Daten
- Erhalt einer Kopie personenbezogener Daten
- Widerspruch gegen die Verarbeitung von Daten für bestimmte Nutzungsarten, wie etwa Marketing oder Profilerstellung
- Verpflichtung der Organisationen, Datenlecks innerhalb von 72 Stunden an die zuständigen Behörden zu melden

Q: Was sind personenbezogene Daten?
A: Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Es gibt keinen Unterschied zwischen privaten, öffentlichen oder beruflichen Rollen einer Person. Persönliche Daten umfassen:

- Name
- E-Mail-Adresse
- Social-Media-Beiträge
- Physische, physiologische oder genetische Informationen
- Medizinische Informationen
- Ort
- Bankdetails
- IP-Adresse
- Cookies
- Kulturelle Identität

Q: Wie können Unternehmen bei Nichteinhaltung bestraft werden?
A: Wenn Unternehmen bestimmte Anforderungen der Datenschutz-Grundverordnung nicht einhalten, können sie Strafen von bis zu 20 Millionen Euro oder 4 Prozent des jährlichen weltweiten Umsatzes erhalten – je nachdem, was höher ist.

Q: Sind die Microsofts Cloud-Dienste mit dem Inkrafttreten der Datenschutz-Grundverordnung weiterhin rechtskonform?
A: Microsoft gewährleistet, dass bis zum Inkrafttreten der Verordnung am 25. Mai 2018 die Microsoft Cloud-Dienste mit der Datenschutz-Grundverordnung rechtskonform sein werden. Das schließt Produkte wie Office 365, Dynamics 365, Microsoft Azure, SQL Server, Enterprise Mobility + Security und Windows 10 ein. Wie auch für die globalen Cloud-Services gewährleistet Microsoft, dass die Angebote aus der Microsoft Cloud Deutschland den Anforderungen der Datenschutz-Grundverordnung entsprechen.
Die Ziele der DSGVO stimmen mit dem bereits seit langem bestehenden Zusagen von Microsoft im Hinblick auf Sicherheit, Datenschutz und Transparenz überein. Microsofts Rechenzentren nutzen weltweit die einheitliche, geprüfte und bewährte Technologien und bieten die gleichen Service-Level und Sicherheitsstandards, z.B. Datenverschlüsselungen nach aktuellen SSL/TLS-Protokollen.

Q: Gilt die Datenschutz-Grundverordnung für Auftragsverarbeiter und die verantwortliche Stelle?
A: Ja, die Datenschutz-Grundverordnung gilt für die verantwortliche Stelle und für Auftragsverarbeiter. Die verantwortliche Stelle ist für die Daten verantwortlich; ein Auftragsverarbeiter verarbeitet die Daten für den Controller. Controller dürfen nur Verarbeiter verwenden, die Maßnahmen ergreifen, um die Anforderungen der Datenschutz-Grundverordnung zu erfüllen. Ein Controller bestimmt, warum und wie persönliche Daten verarbeitet werden, während der Verarbeiter die Vorgänge an persönlichen Daten im Auftrag des Controllers durchführt.
Unter der Datenschutz-Grundverordnung haben die Verarbeiter zusätzliche Pflichten übernommen und haften bei fehlender Einhaltung. Die Pflichten eines konformen Verarbeiters:

- Verarbeiten von Daten gemäß Anweisung
- Verwenden geeigneter technischer und organisatorischer Maßnahmen zur Verarbeitung persönlicher Daten
- Löschen oder Zurücksenden der Daten an den Controller
- Sicherstellen der Berechtigung bei Kontakt mit anderen Verarbeitern

Q: Muss jedes Unternehmen einen Datenschutzbeauftragten benennen?
A: Dies hängt von mehreren gesetzlichen Faktoren ab. Falls das Unternehmen einen Datenschutzbeauftragten ernennen muss, ist dieser verantwortlich für die Information der Mitarbeiter über ihre Compliance-Pflichten sowie für die Durchführung der Überwachung, Schulung und Prüfungen, die gemäß der Datenschutz-Grundverordnung erforderlich sind.

Q: Inwiefern ändert die Datenschutz-Grundverordnung die Anforderungen an die Reaktion einer Organisation bei einer Verletzung des Schutzes personenbezogener Daten?
A: Die Datenschutz-Grundverordnung ändert die Datenschutzanforderungen und verwendet strengere Verpflichtungen für Auftragsverarbeiter und der verantwortlichen Stelle im Hinblick auf Benachrichtigungen bei Verstößen gegen persönliche Datenrechte, die zu einer Gefährdung der individuellen Rechte und Freiheit führen können. Unter der neuen Verordnung muss der Auftragsverarbeiter der verantwortlichen Stelle unverzüglich über einen Verstoß gegen persönliche Datenrechte benachrichtigen, sobald er davon erfährt. Sobald er einen Verstoß zur Kenntnis nimmt,

muss die verantwortliche Stelle die zuständige Schutzbehörde innerhalb von 72 Stunden benachrichtigen. Falls der Verstoß ein hohes Risiko für die Rechte und Freiheit von Einzelpersonen darstellt, müssen die Controller zudem unverzüglich die betroffenen Einzelpersonen verständigen. Microsoft-Produkte und -Dienste wie Microsoft Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, SQL Server-/Azure SQL-Datenbank und Windows 10 bieten Lösungen, die Organisationen beim Erkennen und Bewerten von Sicherheitsbedrohungen und -verstößen sowie beim Erfüllen der Verpflichtungen zur Benachrichtigung bei Verstößen gegen die Datenschutz-Grundverordnung helfen.

Q: Beschäftigt sich die Datenschutz-Grundverordnung mit Verschlüsselung?
A: Verschlüsselung ist in der Datenschutz-Grundverordnung als Schutzmaßnahme anerkannt, mittels derer von einem Datenschutzverstoß betroffene personenbezogene Daten für nicht zum Zugriff berechtigte Personen unzugänglich gemacht werden können. Daher werden die Anforderungen für eine Benachrichtigung über einen Verstoß gegen persönliche Datenrechte beeinflusst – egal ob eine Verschlüsselung verwendet wird oder nicht. Die Datenschutz-Grundverordnung verweist zudem je nach Risiko auf die Verschlüsselung als geeignete technische oder unternehmerische Maßnahme in bestimmten Fällen. Verschlüsselung ist auch eine Anforderung des Payment Card Industry Data Security Standard und Teil der strikten Compliance-Richtlinien, die für die Finanzdienstleistungsbranche gelten. Microsoft-Produkte und -Dienste wie Microsoft Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, SQL Server-/Azure SQL-Datenbank und Windows 10 bieten eine zuverlässige Verschlüsselung von Daten während der Übertragung und ruhenden Daten.

Q: Wie viel kostet die Einhaltung der Datenschutz-Grundverordnung?
A: Die Einhaltung der Datenschutz-Grundverordnung kostet den meisten Organisationen Zeit und Geld; die Umstellung dürfte jedoch reibungsloser für Unternehmen ablaufen, die einen gut strukturierten Cloud-Service verwenden und ein wirksames Programm zur Datenkontrolle haben.

Q: Welche Microsoft-Produkte helfen Unternehmen bei der Einhaltung der Datenschutz-Grundverordnung?
A: Verschiedene Microsoft-Produkte und -Dienste helfen Unternehmen bei der Vorbereitung auf die Einhaltung der Datenschutz-Grundverordnung. Spezifische Informationen finden Sie in den Abschnitten zu Microsoft Azure, Dynamics 365, Enterprise Mobility + Security, Office 365, SQL Server-/Azure SQL-Datenbank und Windows 10.

Die wichtigsten Links im Überblick:

- Webseite der EU zur Datenschutz-Grundverordnung
- Microsoft Deutschland Pressemappe „Trusted Cloud – Microsoft Sichterheit, Datenschutz, Compliance & Transparenz“
- Webinar: „Microsoft on Trust, Privacy and the GDPR“ (englisch)
- Blogbeitrag von Julia White: “Accelerate your GDPR compliance with the Microsoft Cloud” (englisch)
- Blogbeitrag von Brendon Lynch: „Get GDPR compliant with the Microsoft Cloud“ (englisch)
- Ausführliche Anleitung zur Vorbereitung von Unternehmen auf die DSGVO