Die Datenschutz-Grundverordnung ist da – was nun?

Mag. Jordan Georgiev
Geschäftsführer JKG Advisory

Wien, 08. Mai 2018

Daten sind das Öl des 21. Jahrhunderts…

„Democracy – im Rausch der Daten“

Privatsphäre im 21. Jahrhundert…

Die digitale Revolution schreit nach einem neuen Datenschutz-recht – neuer primärrechtlicher Rahmen der EU ermöglicht dies

Alltag im 21. Jahrhundert…

- Domestizierung des Internets
- Verarbeitungen im Web 2.0 (Cloud, AI, …)
- Von Festnetz zum Smartphone – von “heavy user“ bis hin zu Digital Natives
- Einmarsch sozialer Netze und Online-Plattformen
- Grenzüberschreitendes Surfen im Sekundentakt überall und jederzeit (24/7)
- …aber „das Internet vergisst nichts“
- Digitalisierung aller Bereiche unseren Alltags (Blockchain, IoT…)

…Datenschutz aus dem 20. Jahrhundert

- rechtliche Zersplitterung wegen unterschiedlicher Umsetzung der RL 95/46 in den Mitgliedstaaten
- Uneinheitliche Rechtsprechung der Kontrollstellen in den Mitgliedstaaten
- Aufwändiges Registrierungsverfahren
- Komplexe Verfahren bei staatenüber-greifenden Datenanwendungen
- Durchsetzung von Rechten der Betroffenen (z.B. Löschungsanspruch bei Facebook)
- Keine Anwendung im Bereich Justiz und Inneres

Der Schutz personenbezogener Daten in Europa ist weltweit einzigartig als Grundrecht verankert

Artikel 8 der Charta der Grundrechte der EU

Artikel 16 des Vertrags über die Arbeitsweise der EU

Was ist das Neue an der DSGVO?

Zielsetzungen

- einheitlicher Rechtsschutz für alle Betroffenen in der EU
- einheitliche Regeln für die Datenverarbeitung innerhalb der EU
- Gewährleistung eines starken und einheitlichen Vollzuges

- EK-Vorlage Jän 2012 – In Kraft seit Mai 2016 – Geltung ab 25.05.2018
- Rückgrat des allgemeinen DS der EU, einheitlich und unmittelbar anwendbar – 11 Kapitel, 99 Artikel
- Anwendung – Niederlassung oder Verarbeitung in EU oder Datenverarbeitung von Personen in der EU woanders
- Stärkung der Betroffenenrechte – Informationspflichten des Unternehmens, Auskunftsrecht, Recht auf Richtigstellung, Löschung, auf „Datenportabilität“, Verzicht auf “Profiling“ etc.
- Risikobasierter Ansatz – Verlagerung auf Unternehmen (kein Verwaltungsaufwand) und Risikoprüfung der Datenanwendung
- DS-Behörden: Unabhängigkeit (DPA), One-Stop-Shop, Kooperation, EDPB
- 69 „Öffnungsklauseln“ – Spezifikationen, Optionen, Beschränkungen und Ausnahmen, Regelungsverpflichtugen
- Sanktionen (DPAs) + Geldbußen (10-20 Mio./2-4% v Umsatz)

Quelle: DSGVO

Vorurteil 1: Zu wenig Zeit für die Anpassung an die DSGVO

Entwicklung des Datenschutzes

1981	DS-Konvention des Europarates
1995	DS-Richtlinie der EU
2000	DSG 2000
2009	Grundrechtecharta der EU, Artikel 8
2012	EK-Vorlage DSGVO
2016	DSGVO in Kraft
2018	DSGVO in Geltung

Kommentare

- Datenschutz ist seit den 80er ein wichtiges Thema in Europa
- Die Datenschutz-Richtlinie ist seit 1995 in Kraft und entspricht zu 2/3 der DSGVO
- DS-RL beinhaltet ähnliche Verpflichtungen für die Unternehmen, aber ohne Sanktionen
- Österreich setzte mit dem DSG 2000 die DS-RL mit dem höchstmöglichen Standards in Europa um
- Seit 2012 liefen die Diskussionen, seit 2016 ist die DSGVO verabschiedet und in Kraft

Vorurteil 2: Zu viel Aufwand, um DSGVO-compliant zu sein

Auflagen der DSGVO	Notwendige Schritte
• Keine allg. Vorabkontrollen oder Meldungen an das DVR, dafür aber Verzeichnis der Verarbeitungstätigkeiten führen	• Verarbeitungsverzeichnis ist mit gängigen IT-Mitteln (Datenbanken) leicht realisierbar
• Rechtsgrundlege der DV (Einwilligung, Vertrag)	• Einwilligung einholen (one-off effort)
• Nicht Unternehmensgröße (250 MA), aber Risiken und Auswirkungen der Datenverar-beitung ausschlaggebend	• „Know your data“ – besonderer Schutz bei sensiblen Daten, Video-überwachung (vs Image-Verlust)
• Datenschutz-Folgenabschätzung (DPIA) und Konsultationspflicht mit DPA	• Wenn nicht high-risk (system. Bewer-tung pers. Aspekte) – kein DPIA
• Datenschutzbeauftragter (DPO) soll bestellt werden (abhängig von Kerntätigkeit der DV)	• Bereits Teil der IT-Organisation, hoch angesiedelt, joint-DPO möglich
• Datenschutz „by design or by default“ - Dokumentationspflichten und Sicherheit der Datenanwendungen	• Schritt von Security zu Privacy ist nicht zu groß – Kenntnis über Daten und Systeme ist kritisch
• Rechte der Betroffenen gewährleisten (Auskunft, Berichtigung, Löschung…)	• Müssen in Betriebsprozessen verankert werden (one-off effort)

Vorurteil 3: Die DSGVO zerstört bestehende Geschäftsmodelle

Vertrauen als Wachstumspotential	• Über 50% der Menschen in der EU haben kein Vertrauen in Digitaldienste (Internet) und verwenden diese nicht oder zu wenig (Eurobarometer)
Datenschutz als Geschäftsmodell	• „Server liegt in der EU“ • Verschlüsselung und datenschutzfreundliche Voreinstellung • DPO als Beruf (weltweit Bedarf für 75.000 DPOs, IAPP)
Wettbewerbsvorteil für Österreich	• DSG 2000 bereits als hoher Standard • Potential für österreichische spezialisierte Anbieter und KMUs
DSGVO als globaler Standard	• Südkorea, Japan, Brasilien wollen Abkommen mit der EU und setzen DSGVO-Standards national um) • Große Konzerne setzen DSGVO-Standards für ihre Produkte und Dienste weltweit um

Beispiel: Wie kann man als Verein DSGVO implementieren

Mitgliederverwaltung	• Einwilligung zur DV einholen (aktiv bei Anmeldung als Mitglied), im Nachhinein für bestehende Mitglieder • Verarbeitungshistorie (Verzeichnis) über Datenbank • Selbstverwaltung der Personendaten (Mein Profil)
Newsletter und Events	• Aktive Anmeldung durch Mitglieder • Abbestellung Newsletter sofort per Mausklick • Zustimmung zur Verwendung von Eventfotos auf Homepage
Datenschutz-Folgeabschätzung	• **Nicht notwendig**, da kein hohes Risiko bei der DV im Verein besteht • Nur die notwendigsten Daten werden erhoben
Datenschutzbeauftragter	• **Nicht notwendig**, da nur 3 Personen mit personenbezogenen Daten regelmäßig umgehen

Anmerkung: Diese Darstellung soll nur als Beispiel und nicht als Anleitung dienen. Jeder Fall soll sorgfältig im Sinne des DSGVO geprüft werden.

office@jkg-advisory.com
www.jkg-advisory.com