VÖW-Sommermeeting 2017

Wie schützen Sie Ihre sensiblen Daten im digitalen Zeitalter?

corporate identity prihoda gmbh

peter-jordan str. 74
1190 wien

tel.: +43 (1) 47 96 366-10
office@cip.at

www.cip.at

Die neue Datenschutz-Grundverordnung (DSGVO): Auswirkungen auf Österreich

Autor: Mag.jur. Thomas Wohlesser
Senior Legal Counsel bei Atos IT Solutions and Services GmbH

Agenda

1. Allgemeines
2. Anwendungsbereich
3. Sanktionen bei Nichteinhaltung des Datenschutzrechtes
4. Meldepflichten
5. Datenschutz-Folgenabschätzung
6. Datenschutzbeauftragter
7. Rechte der Betroffenen
8. Erweiterte Haftung für Verantwortliche und für Auftragsverarbeiter
9. Erleichterter Datenaustausch im Unternehmen
10. Zustimmung vs. Einwilligung
11. Zusammenfassung

Allgemeines

- Verordnung [EU] 2016/679 (Datenschutz-Grundverordnung)
- Aufhebung der Richtlinie 95/46/EG (Datenschutzrichtlinie)
- Anwendbarkeit
  - in jedem EU-Mitgliedsstaat unmittelbar anwendbar (Ziel: Vereinheitlichung des EU-Datenschutzrechtes)
  - Änderung des österr. Datenschutzgesetzes 2000 (noch kein Entwurf veröffentlicht)
  - Öffnungsklauseln: Spielräume für die Mitgliedsstaaten
- Ab 25. Mai 2018 in Geltung

Anwendungsbereich

DSG 2000	DSGVO
Personenbezogene Daten • Natürliche Personen • Juristische Personen	Personenbezogene Daten • Natürliche Personen

Auswirkungen in Österreich

- Wesentliche Erleichterung bei der Verarbeitung von Daten von juristischen Personen (Bsp.: Rechnungslegung)
- Achtung: Mitarbeiter von Unternehmen, Ein-Personen-Unternehmen

Globale Anwendung der DSGVO

- Räumlicher Anwendungsbereich des EU-Datenschutzrechts massiv erweitert
  - **Datenverarbeitung im Rahmen von Tätigkeiten einer Niederlassung** eines Verantwortlichen oder Auftragsverarbeiters in der Union (entscheidend ist dabei der Ort der Niederlassung und nicht der Ort der Datenverarbeitung)
  - **„Marktortprinzip“** – auch auf Verantwortliche oder Auftragsverarbeiter ohne Niederlassung in der EU anwendbar

DSGVO gilt für Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung...

  - dazu dient, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten.
  - das Verhalten betroffener Personen beobachtet, soweit ihr Verhalten in der Union erfolgt.

Sanktionen bei Nichteinhaltung

DSG 2000	DSGVO
Verwaltungsstrafen bis zu 25.000 Euro	• Kartellrechtsniveau • 2 Stufen ✓ einerseits bis 10 Millionen Euro oder 2 % des konzernweiten Umsatzes ✓ andererseits bis 20 Millionen Euro oder 4 % des konzernweiten Umsatzes

Auswirkungen in Österreich

- Internes Risikomanagement
- Konzernweites DMS

Meldepflichten

DSG 2000	DSGVO
Meldepflicht bei Datenschutzbehörde (Datenverarbeitungsregister)	**Erweiterte Nachweispflichten (Accountability)** • Rechenschaftspflicht • Risikobasierter Ansatz • Verzeichnis von Verarbeitungstätigkeiten • Privacy by design • Privacy by default

Auswirkungen in Österreich

- Interne Dokumentationspflichten
  - Verarbeitungstätigkeiten, Dienstleisterverträge
- Datenschutz durch Technikgestaltung

Datenschutz...

... durch Technik und datenschutzfreundliche Voreinstellungen

- Der Verantwortliche muss nachweisen können, dass er Datenschutzgrundsätze einhält.
- Auftragsverarbeiter müssen dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, damit der Verantwortliche nachweisen kann, dass er seine Pflichten erfüllt.
- Art. 25 DSGVO regelt den Grundsatz der **„privacy by design“** bzw. die Anforderung **„privacy by default“**: Unternehmen müssen ihre IT-Systeme grundsätzlich so ausgestalten, dass sie nur gerade so viele Daten erheben, wie zur Erfüllung des verfolgten Zwecks erforderlich ist.
- IT-Systeme sollen so „voreingestellt“ sein, dass sie grundsätzlich nur die erforderlichen personenbezogenen Daten verarbeiten.

Meldung bei Datensicherheitsvorfällen I

Data Breach Notification Duty

DSG 2000 (§ 24)	DSGVO
Wenn bekannt ist, dass Daten systematisch und schwerwiegend unrechtmäßig verwendet wurden und dem Betroffenen ein Schaden droht: • Betroffene **unverzüglich** in geeigneter Form informieren • **Außer:** bei geringfügigen Schäden oder unverhältnismäßig hohem Kostenaufwand	• **unverzüglich**, ohne unangemessene Verzögerung/max. **72h** Meldung an DSB • **Ausnahme:** (keine Pflicht zur Meldung bei DSB, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt.) • Meldung an Betroffene wenn voraussichtlich hohes Risiko für Rechte und Freiheiten • Vorsatz & Fahrlässigkeit gleichermaßen umfasst

Meldung bei Datensicherheitsvorfällen II

Data Breach Notification Duty - Meldung

DSGVO

Meldung zum „Data Breach“ muss folgende Informationen enthalten:

- Beschreibung der Verletzungsart (Vernichtung, Verlust, Veränderung, unbefugte Offenlegung)
- Angaben zu den Betroffenenkategorien und der ungefähren Zahl der Betroffenen
- Angaben zu den Kategorien und der ungefähren Zahl der betroffenen Daten (z.B. Gesundheitsdaten)
- Name und Kontaktdaten des DPO/Verantwortlichen
- Beschreibung der Folgen
- Beschreibung der Maßnahmen zur Behebung der Verletzung und zur Abmilderung der Folgen der Betroffenen

Achtung: stufenweise Nachmeldung wenn nicht alle Faktoren bekannt sind (aber Mindestangaben anführen)

Meldung bei Datensicherheitsvorfällen III

Data Breach Notification Duty - Auftragsverarbeiter

DSGVO

Auftragsverarbeiter hat geminderte Meldepflichten

- Keine unmittelbare Meldepflicht gegenüber Datenschutzbehörde
- Unverzügliche Informationspflichten gegenüber Verantwortlichen
- Unterstützungspflicht des Auftragsverarbeiters gegenüber Verantwortlichen

Meldung bei Datensicherheitsvorfällen IV

Data Breach Notification Duty – Sanktionen und Maßnahmen

DSGVO

Sanktionen

- Bei Verstößen gegen Melde- und Benachrichtigungspflichten drohen Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres
- Eventuelle materielle und immaterielle Schäden bei nicht rechtzeitiger oder angemessener Reaktion – Schadenersatzverfahren

Maßnahmen:

- Notfallplan (rechtlich, technisch, Kommunikation)
- Verantwortlicher
- Dokumentation

Datenschutz-Folgenabschätzung statt Vorabkontrolle

Weitergehende Prüf- und Abstimmungspflichten

DSG 2000	DSGVO
Vorab-Kontrolle durch die Datenschutzbehörde bei (Verarbeitung von)… • „sensiblen Daten“ • strafrechtlich relevanten Daten • Daten betreffend Kreditwürdigkeit • dem Informationsverbundsystem • der Videoüberwachung	Datenschutz-Folgeabschätzung (Privacy Impact Assessment) bei Datenverarbeitungen, die voraussichtlich hohes Risiko für Rechte und Freiheiten zur Folge haben.

Auswirkungen in Österreich

- Konsultation mit DSB
- Dokumentation/Information
- Technischer Datenschutz

Datenschutz-Folgenabschätzung

- Das Konzept der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO weicht erheblich von dem der Vorabkontrolle ab.
  - wenn Datenverarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der davon betroffenen Personen zur Folge hat
  - insbesondere Bewertung der Eintrittswahrscheinlichkeit und Schwere möglicher Risiken
  - zusätzlich: Art, Umfang, Umstände, verfolgte Zwecke sowie Ursachen möglicher Risiken bewerten
    (auch Maßnahmen, Garantien und Verfahren prüfen, mit denen bestehende Risiken eingedämmt und die sonstigen Vorgaben der Verordnung eingehalten werden können)
  - Sofern Datenschutz-Folgenabschätzung ergibt, dass die geplante Datenverarbeitung tatsächlich ein hohes Risiko zur Folge hätte, die zuständige Aufsichtsbehörde zu Rate ziehen, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden

Datenschutzbeauftragter

DSG 2000	DSGVO
• Kein verpflichtender Datenschutzbeauftragter in Österreich • Freiwillige Bestellung möglich	Verpflichtende Bestellung für Verantwortliche **und** Auftragsverarbeiter für • **Öffentliche Stellen** • **Unternehmen deren Kerntätigkeit** i. in der Verarbeitung von Daten besteht, die nach Art, Umfang u/o Zweck eine umfangreiche, regelmäßige und systematische Kontrolle von betroffenen Personen beinhaltet oder ii. in der umfangreichen Verarbeitung „besonderer Kategorien von Daten“ oder Daten über strafrechtliche Verurteilungen/Straftaten liegt • Weitere Verpflichtung nach Recht der Mitgliedsstaaten möglich

Zustimmung vs. Einwilligung

DSG 2000	DSGVO
Zustimmung • ohne Zwang • für den konkreten Fall • in Kenntnis der Sachlage (auch konkludent) abgegebene Willenserklärung	Einwilligung • freiwillig • für den bestimmten Fall • in informierter Weise und • unmissverständlich abgegebene Willenserklärung

Auswirkungen in Österreich

- Nachweispflicht

Rechte der Betroffenen

DSG 2000	DSGVO
• Informationspflicht • Recht auf Auskunft • Recht auf Richtigstellung • Recht auf Löschung	**Erweiterte Informationspflichten bei Datenerhebung insbesondere:** • Angabe der Rechtsgrundlage (Einwilligung/ Vertrag/spezifisches berechtigtes Interesse) • Zweckänderung • Recht auf „Vergessen werden“ (bei veröffentlichten Daten und Löschungsanspruch) • Recht auf Datenübertragbarkeit • Automatisierte Einzelentscheidungen (inkl. „Profiling“) • Transparenzgrundsatz

Auswirkungen in Österreich

- Korrespondierende Pflichten des Verantwortlichen
- Adaptierte Prozesse
- Technischer Datenschutz

Transparenzgrundsatz bei Datenverarbeitung

- **Transparenzgrundsatz:** Künftig müssen Unternehmen betroffene Personen deutlich umfassender als bislang und in einer nachvollziehbaren Weise darüber informieren, wie sie deren Daten verarbeiten.

„Die verantwortliche Person muss die betroffenen Personen von der Verarbeitung ihrer personenbezogenen Daten ‚in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer einfachen und klaren Sprache' davon unterrichten."

Erweiterte Haftung
für Verantwortliche und Auftragsverarbeiter

DSG 2000	DSGVO
• DL haftet bei schuldhafter und gesetzwidriger Datenverwendung • strafrechtlich (Freiheitsstrafe bis zu einem Jahr) oder verwaltungsrechtlich (Verwaltungsstrafen bis zu 25.000 Euro) • AG ist grs. verantwortlich	• zivilrechtliche Haftung wegen tatsächlichen oder behaupteten Datenschutzverstößen • **materielle** und **immaterielle Schäden** • Eine weitere Neuerung ist die ausdrückliche Erweiterung der Haftung auch auf **Auftragsverarbeiter**, Art. 82 Abs. 1 DSGVO.

Erleichterter Datenaustausch im Konzern

- **One-Stop-Shops** für Konzerne
  - die für die Hauptniederlassung zuständige Datenschutzbehörde fungiert als "federführende Behörde" für Verarbeitungen mit Auswirkungen auf mehrere Mitgliedstaaten
  - gilt nur bei grenzüberschreitenden Datenverarbeitungen

- Betroffene haben das Beschwerderecht bei der Behörde des Wohnsitzes oder des Arbeitsplatzes (lokale Zuständigkeit)
- Ansonsten – nach wie vor kein ausdrücklich geregeltes "Konzernprivileg"
  - Die Mitgliedstaaten dürfen eigene Regelungen treffen

Zusammenfassung

- Die DSGVO bringt gegenüber dem DSG 2000 erhebliche Veränderungen!
  - Unternehmen müssen zusätzliche Anforderungen erfüllen und die notwendigen Veränderungen zeitnah umzusetzen
  - Dies erfordert vor allem die Anpassung von Arbeitsabläufen und anderen Prozessen, IT- Systemen und Strukturen der Datenverarbeitung
  - Schwerpunkte liegen dabei auf Transparenz und Dokumentation

Vielen Dank

corporate identity prihoda gmbh

peter-jordan str. 74
1190 wien

tel.: +43 (1) 47 96 366-10
office@cip.at

www.cip.at