MOORE STEPHENS

Gesetzlicher Datenschutz

Datenschutzgrundverordnung - Informationssicherheitsmanagement

Datenschutzgrundverordnung (DSGVO)

Gesetzlicher Datenschutz

Mit in Kraft treten des neuen Datenschutzgesetzes mit Mai 2018 werden die Anforderungen an Unternehmen und deren Leitungsorgane signifikant erhöht sowie Verstöße gegen die Bestimmungen unter empfindliche Strafen gestellt

Neue gesetzliche Anforderungen an den Datenschutz in Unternehmen

Der Einsatz von Informationstechnologien ist heutzutage für wachsende und innovative Unternehmen nicht mehr wegzudenken. Beispiele der Vergangenheit zeigen wie gravierend sich Sicherheitsvorfälle (dh. Verlust von Vertraulichkeit oder Integrität oder Verfügbarkeit) in einem Unternehmen darstellen können und mit welchem wirtschaftlichen Schaden oder Reputationsverlust dies verbunden sein kann. Vorstände, Aufsichtsräte und Geschäftsführer sind persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich. Daraus zeigt sich wie wichtig Maßnahmen zum Schutz der eingesetzten Technologien sind.

Ein angemessenes Sicherheitsniveau zu erreichen bzw. aufrecht zu erhalten ist im Alltag für Unternehmen kaum umzusetzen. Mitverantwortlich dafür sind enge Budgetvorgaben, knappe Ressourcen und nicht zuletzt der stetig wachsende Grad an Digitalisierung und Vernetzung.

Worum es geht

Am 25. Mai 2017 trat die EU-Verordnung Nr. 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung oder „DSGVO“) in Kraft. Dadurch begann ein zweijähriger Prozess für Unternehmen, die Verordnungsinhalte bis 25. Mai 2018 anzuwenden.

Wen es betrifft

Die DSGVO dient vor allem dem Schutz natürlicher Personen innerhalb der Europäischen Union hinsichtlich ihres Grundrechtes auf Schutz personenbezogener Daten. Sie vereinheitlicht die Regelungen für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit. Darunter fällt die Verarbeitung und der freie Verkehr personenbezogener Daten durch in der EU ansässige datenverarbeitende, juristische Personen, in der Diktion der DSGVO als „Verantwortliche“ bezeichnet, sowie datenweiterverarbeitende Unternehmen. Darüber hinaus werden auch Unternehmen außerhalb der EU erfasst die personenbezogenen Daten von EU-Bürgern weiterverarbeiten.

Somit erstreckt sich der räumliche Anwendungsbereich sowohl auf Verantwortliche und Auftragsverarbeiter mit Sitz in der EU als auch auf Verantwortliche und Auftragsverarbeiter ohne Sitz in der EU, welche personenbezogene Daten über Personen, die sich in der EU aufhalten, verarbeiten.

Unternehmen müssen eine Vielzahl an Neuerungen berücksichtigen:

- Stärkung der Betroffenenrechte (mehr Transparenz; Verankerung des Rechts auf Vergessenwerden; Einwilligung gilt nur falls freiwillig, aktiv und eindeutig)
- Verstärkte Dokumentationspflichten, die Implementierung weiterer technischer und organisatorischer Maßnahmen
- Neuer Fokus auf die Datensicherheit (verpflichtende angemessene Sicherheitsvorkehrungen; Datenmissbräuche und Sicherheitsverletzungen müssen den Aufsichtsbehörden gemeldet werden)
- Bestellung von Datenschutzbeauftragten im öffentlichen Bereich
- Datenschutzfolgeabschätzung, die auf Risikoanalysen basiert
- Erhöhter Strafrahmen: Strafen von bis zu 20 Millionen Euro beziehungsweise 4 Prozent des Konzernumsatzes

Was sind personenbezogene Daten

Die DSGVO regelt die ganz oder teilweise automatisierte Verarbeitung von personenbezogenen Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Das Dateisystem kann automatisiert oder manuell geführt werden.

Dies bedeutet, dass alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen in das Regelungsregime der DSGVO fallen. Definitionsgemäß ist zwischen „personenbezogenen Daten" und sogenannten „besonderen personenbezogenen Daten" zu unterscheiden.

Personenbezogene Daten

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (zB. Name, Adresse, SV-Nr.).

Besondere Kategorien personenbezogener Daten

Umfasst sind hier Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Wann können Daten rechtmäßig verarbeitet werden

Die Verarbeitung ist rechtmäßig wenn gem. Art 6 Abs. 1 DSGVO nachfolgende Vorgaben erfüllt sind:

- Vorliegen der Einwilligung der betroffenen Person
- Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen
- Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen
- Schutz lebenswichtiger Interessen,
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder
- aufgrund einer Interessenabwägung erforderlich ist

Was heißt das für ihr Unternehmen

Die neuen Verpflichtungen zum Umgang mit personenbezogenen Daten führen zur weitreichenden Neuerungen für die Unternehmen. Die Anforderungen umfassen dabei neben dem Datenschutz auch organisatorische Maßnahmen, die je nach Ausgestaltung sämtliche Bereiche des Unternehmens umfassen. Die Ansprüche der DSGVO lassen sich wie auf der Nebenseite tabellarisch dargestellt zusammenfassen. Diese Maßnahmen sind nachvollziehbar zu dokumentieren, um hier - wo gesetzlich erforderlich - zeitnahe und standardisiert Auskünfte zu erteilen.

Was sind die Konsequenzen bei Nichteinhaltung der DSGVO?

Mit Inkrafttreten wurden auch die Befugnisse der Aufsichtsbehörde, in Österreich die „österreichische Datenschutzbehörde" (vormals: Datenschutzkommission), erweitert. Verstöße können je nach Art, Schwere, Dauer des Verstoßes und Ausmaß des erlittenen Schadens bis zu 20 MEUR oder bis zu 4% des weltweiten Jahresumsatzes betragen. In Österreich ist im Gesetz auch eine Verwaltungsstrafe iHv 50 TEUR vorgesehen sofern die Tat nicht nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

Anforderungen des Datenschutzgesetzes an Unternehmen		
(a)	**Privacy by Design und Privacy by Default**	
	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen; es sind geeignete technische und organisatorische Maßnahmen und Verfahren (zB Pseudonymisierung) zu treffen. Sicherstellung, dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.	
(b)	**Führen eines Verzeichnisses der Verarbeitungstätigkeiten**	
	Die Meldung hat dabei insbesondere nachfolgende Informationen gemäß Art 30 DSGVI zu enthalten:	
	(i)	die eigenen Kontaktdaten des Unternehmens
	(ii)	eine Beschreibung die Zwecke der Verarbeitung
	(iii)	eine Beschreibung der Datenkategorien und der Kategorien von betroffenen Personen und Empfängerkategorien
	(iv)	eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen
(c)	**Meldungen an die Datenschutzbehörde bei Datenschutzverletzungen**	
	Verletzungen des Schutzes personenbezogener Daten sind sowohl den nationalen Aufsichtsbehörden (binnen höchstens 72 Stunden nach dem Entdecken) als auch der betroffenen Person mitzuteilen	
(d)	**Durchführung einer Risikobewertung im Sinne der Datenschutz-Folgenabschätzung**	
	Im Falle eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen besteht die Pflicht zur Datenschutz-Folgenabschätzung, die zumindest nachfolgende Inhalte zu umfassen hat	
	(i)	Beschreibung der geplanten Verarbeitungsvorgänge
	(ii)	Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
	(iii)	Bewertung der Risiken für die Rechte der Freiheiten der betroffenen Personen
	(iv)	Geplante Abhilfemaßnahmen zur Begegnung der Risiken, sowie Garantien, Sicherheitsvorkehrungen und Verfahren
(e)	**Sicherstellen kurzer Auskunftszeiten für Meldungen an Betroffene (Recht auf Auskunft, Löschung, Richtigstellung, Datenübertragbarkeit, Widerspruch)**	

(Fortsetzung)		
(f)	**Pflicht zur Bestellung eines Datenschutzbeauftragten („DSB") besteht**	
	(i)	Soweit die Kerntätigkeit des Unternehmens eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen umfasst bzw.
	(ii)	die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht.
	Der Datenschutzbeauftragte („DSB") kann ein Arbeitnehmer als auch ein Selbständiger (Externer) sein. Dabei muss die Person über die geeignete Qualifikation und dem für die Position entsprechenden Fachwissen verfügen. Darüber hinaus ist der DSB weisungsfrei und hat unmittelbar an die höchste Managementebene zu berichten.	
(g)	**Neue Informationspflichten und Betroffenenrechte**	
	Im Rahmen der Umsetzung der DSGVO werden auch die Rechte und Informationspflichten der Betroffenen deutlich ausgeweitet. Dies kann bei den Verantwortlichen und Verarbeitern personenbezogener Daten aufgrund der inhaltlichen und zeitlich eingeschränkten Auskunftspflichten organisatorische Umstrukturierungen und Adaptierungen in der IT-Struktur erfordern. Die Informationspflichten und Betroffenenrechte gem. DSGVO lassen sich wie folgt darstellen, wobei Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können. Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden:	
	(i)	Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber innerhalb eines Monats zu erledigen (diese Frist kann um höchstens weitere 2 Monate verlängert werden)
	(ii)	Auskunftsrecht (ua über geplante Speicherdauer)
	(iii)	Recht auf Berichtigung
	(iv)	Recht auf Löschung und auf „Vergessenwerden"
	(v)	Recht auf Einschränkung der Verarbeitung
	(vi)	Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger
	(vii)	Recht auf Datenübertragbarkeit
	(viii)	Widerspruchsrecht
	(ix)	Regelungen betreffend automatisierte Generierung von Einzelentscheidungen einschließlich Profiling

Datenschutzgrundverordnung (DSGVO)

Typische Fragestellungen

Gerne helfen wir Ihnen nicht nur bei den nachfolgenden Fragen, die sich vielen Unternehmen stellen, weiter:

Q: Wir führen die Lohnverrechnung selbst in unserem Unternehmen durch: welche neuen Risiken treffen uns?

Q: Können wir uns gegen externen Datendiebstahl so absichern, dass uns keine Haftung trifft?

Q: Wie bestimmen wir unsere Risikoklasse und wie dokumentieren wir eingeholte Zustimmungen?

Q: Berufsrechtliche Vorschriften erfordern die Einholung von Ausweisdaten: welche Anforderungen ergeben sich?

Q: Aus der Bestellhistorie unserer Kunden ergeben sich zwangsläufig auswertbare Gesundheitsdaten: welche Auswirkungen hat das?

Q: Unser Unternehmen hat bereits eine DVR-Nummer. Hat die DSGVO auch auf uns Auswirkungen?

Q: Wir sind nur ein kleines Unternehmen. Gibt es opting-out oder de-minimis Bestimmungen, unter die wir fallen könnten?

Unsere Zusammenarbeit

Moore Stephens blickt in den Bereichen IT, IT Audit sowie IT Sicherheit auf eine jahrelange erfolgreiche Zusammenarbeit mit Grünberger IT-Consulting zurück. Auch im Bereich Datenschutzgrundverordnung sowie Datensicherheit setzen wir diese Zusammenarbeit fort.

Unser Leistungsangebot

- Informationssicherheits- und Datenschutzberatung samt Identifikation von personenbezogenen Daten
- Etablierung eines Datenschutz-Managementsystems samt unternehmensweiter Datenschutzstrategie; Erstellung eines Handbuch und Identifikation der Notwendigkeit eines Datenschutzbeauftragten
- Durchführung von IT- und Informationssicherheit-Audits Aufbau eines ISMS nach ISO/IEC 27001
- Schulung und Coaching CISO
- Externer CISO
- Aufbau eines IT-Governance Frameworks nach COBIT 5
- Business Continuity Management
- Risikobewertung nach ISO 31000

Externe Datenschutzbeauftragte

Übernahme der Funktion des Datenschutzbeauftragen für Unternehmen:

- Beratungssicherheit durch einen zertifizierten externen Datenschutzbeauftragten
- Kompetenter Ansprechpartner auf kurzem Wege
- Laufende Beratung und kurzfristige Reaktion bei neuen Anforderungen
- Überwachung der Dokumentation und der Risikobewertung
- Durchführung laufender Datenschutz-Audits

Über Moore Stephens

Moore Stephens Interaudit und Moore Stephens Salzburg zählen gemeinsam mit ihren Standorten in Salzburg, St. Pölten und Wien zu den großen regionalen Wirtschaftsprüfungs- und Steuerberatungsgesellschaften und bieten ein breites Spektrum an branchenübergreifenden Dienstleistungen an.

Die langjährige Erfahrung unserer Partner in internationalen Prüfungsgesellschaften im In- und Ausland in leitenden Positionen, die auch die Betreuung von Kunden in regulierten und kapitalmarktorientierten Bereichen umfasst, ist die Grundlage für unseren kompromisslos qualitätsorientierten Zugang. Die Mitgliedschaft in einem der zehn größten weltweit tätigen Wirtschaftsprüfungs- und Beratungsnetzwerke schafft Kompetenz für die qualitativ hochwertige Betreuung unseres internationalen Kundenkreises.

Unsere lokale Verbundenheit ermöglicht es uns, unserem regionalen Kundenkreis ein auf Größe und Geschäftsumfang angepasstes Leistungsspektrum von höchster Qualität zu erbringen.

Moore Stephens weltweit

Moore Stephens Interaudit und Moore Stephens Salzburg sind Partner der Moore Stephens International Limited – einem Netzwerk von über 300 führenden unabhängigen Wirtschaftsprüfungs- und Beratungsfirmen mit aktuell 660 Büros in 105 Ländern. Damit zählt die Moore Stephens - Gruppe zu den zehn weltweit größten Wirtschaftsprüfungs- und Beratungsnetzwerken.

Kontaktinformationen

Für weitere Informationen zu den in dieser Broschüre dargestellten Inhalten oder Informationen zu unseren Serviceleistungen kontaktieren Sie bitte:

Herbert Huber – Partner
herbert.huber@moorestephens.at

Christopher Bohac - Senior Manager
christopher.bohac@moorestephens.at

Paul Grünberger CISA, CISM, CRISC, Zertifizierter Datenschutzbeauftragter (CIS) - Grünberger IT-Consulting
paul@gruenberger.org

Moore Stephens Interaudit Wirtschaftsprüfung GmbH
Moore Stephens Salzburg GmbH

interaudit.moorestephens.com
salzburg.moorestephens.com

A-5020 Salzburg, Innsbrucker Bundesstraße 126
T +43 (662) 251 500-0

A-1010 Wien, Kärntner Ring 5-7, 6. Stock
T +43 (1) 312 111

A-3100 Sankt Pölten, Jahnstrasse 19
T +43 (2742) 79 789-0

MOORE STEPHENS