

Computerpartner

Sie befinden sich hier: **HOME** → **Nachrichten** → **Aktuell** → **News**

06.11.2017

DSGVO: Die Uhr tickt immer lauter

Als allgegenwärtiges Schlagwort sorgt die DSGVO seit rund zwei Jahren für Kopfschmerzen bei Entscheidungsträgern und IT-Verantwortlichen. Unternehmen jeder Branche und Größe werden dann stärker in die Pflicht genommen, personenbezogene Daten zu schützen.

Mathias Hein

Viel Zeit bleibt dafür nicht mehr: Am 25. Mai 2018 tritt die neue EU-Datenschutz-Grundverordnung (DSGVO) in Kraft. Wie Unternehmen ihre Organisation rechtlich und technisch fit für die DSGVO machen können, wurde am Dienstag im Rahmen einer Informationsveranstaltung von S&T und LANSKY, GANZGER + partner diskutiert und aufgezeigt. Mehr als 90 Gäste folgten der Einladung in die Kanzleiräumlichkeiten in der Wiener Innenstadt.



Harald Leitenmüller

© quelle microsoft

Europaweit setzen sich Unternehmen mit dem Thema Datenschutz intensiv auseinander. Anlass ist die Datenschutz-Grundverordnung der Europäischen Union (DSGVO), die im Vorjahr beschlossen wurde und am 25. Mai 2018 in Kraft tritt. Spätestens dann wird sich in vielen Unternehmen zeigen, ob die vorhandenen Sicherheitsmechanismen funktionieren und betriebliche Konzepte den neuesten technischen und rechtlichen Anforderungen entsprechen und welche Versäumnisse in puncto Daten- und Informationssicherheit nachgeholt werden müssen. Die Sanktionen bei Nichteinhaltung der DSGVO sind empfindlich. Es können Geldbußen von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweit erzielten Jahresumsatzes verhängt werden. Im Fall von Schadenersatzklagen gelten die Prinzipien der Beweislastumkehr und der Solidarhaftung. Unternehmen stehen in Zukunft unter genauer Beobachtung der Datenschutzbehörden.

IN ZEHN SCHRITTEN ZUR DATENSCHUTZ-COMPLIANCE

Der Countdown läuft – dennoch gilt es einen kühlen Kopf zu bewahren, wie **Dr. Gerald Ganzger, Rechtsanwalt und Managing Partner bei LANSKY, GANZGER + partner**, eindringlich erläuterte. Der bekannte Jurist, der regelmäßig Kolumnen für die Branchenzeitschrift "Horizont" zum Medien- und IP-Recht sowie zu allen Fragen des Persönlichkeitsschutzes, einschließlich Datenschutz schreibt, stellte den Gästen einen 10-Punkte-Plan für die Einhaltung der DSGVO vor. Dazu zählen: Erhebung des Status der derzeitigen Datenverarbeitung, Einrichtung eines Datenschutz-Compliance-Systems, Bestellung eines Datenschutzbeauftragten, Überprüfung der Datenschutzzustimmungserklärungen, Überprüfung der bisher verwendeten Formulare, Errichtung eines Kontrollsystems, Einrichtung eines Dokumentationssystems, Überprüfung der Verträge mit Auftragsverarbeitern, Datenschutz durch Technik sowie Information der Mitarbeiter und Schulungen. Wichtig ist es laut Dr. Ganzger, sich umfassend beraten zu lassen, sich aber dennoch selbst proaktiv mit der Datensicherheit im eigenen Unternehmen zu befassen.

Privacy by Design. Privacy by Default.

Ing. Mag. Amra Bajraktarevic, Netzwerkexpertin und Rechtsanwaltsanwältin mit Spezialisierung auf Datenschutz, gab in ihrem Vortrag einen kompakten Überblick über die Grundsätze der Datenverarbeitung: Rechtmäßigkeit der Verarbeitung, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit der Datenverarbeitung, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht. Dass die Einhaltung der DSGVO vor allem von der Technikgestaltung des jeweiligen Unternehmens abhängt, wurde den Gästen anhand der beiden Prinzipien "Privacy by Design" und "Privacy by Default" aufgezeigt. Die DSGVO setzt voraus, dass technische Systeme in Unternehmen auf rechtskonforme Datenverarbeitung ausgelegt sind ("Privacy by Design"). Zudem sind zum Schutz der Betroffenen Standardeinstellungen datenschutzfreundlich zu gestalten ("Privacy by Default"). Das Prinzip sieht keine Verhältnismäßigkeitsprüfung vor, es ist also unabhängig von den Kosten oder Risiken umzusetzen. Da die Pflicht zu datenschutzfreundlichen Voreinstellung auch für bestehende Systeme gilt, empfiehlt sich deren rasche Überprüfung, etwa im Zuge laufender Updates, und Vereinbarungen mit Zulieferern.

3,2,1... - MEINS!

Wie simpel es für Cyberkriminelle sowie auch Auslandsgeheimdienste ist, in Firmennetzwerke einzudringen oder personenbezogene Daten abzufangen, wurde den Gästen anhand eines Live-Hackings von **Dr. Stefan Schiebeck, seines Zeichens zertifizierter ethischer Hacker am Center for Digital Safety & Security des AIT Austrian Institute of Technology**, demonstriert. Die schier unüberschaubare, stetig wachsende Zahl an Datenpannen in der jüngsten Vergangenheit zeigt, dass kein Unternehmen vor Angriffen gefeit ist, wenn die grundlegenden Prinzipien des Datenschutzes nicht eingehalten werden. Besonders heikel wird es in Hinblick auf die Verarbeitung personenbezogener Daten, die ein hohes Risiko für die betroffenen Personen darstellen, dazu zählen etwa strafrechtliche Daten. Daher müssen Unternehmen gemäß DSGVO eine sogenannte Datenschutz-Folgeabschätzung, eine systematische Beschreibung über die Verarbeitungsprozesse und Zwecke, eine Beurteilung über die Risiken für Betroffene sowie Maßnahmen zum Schutz der Daten enthalten.

INFORMATIONSPFLICHTEN GEGENÜBER "BETROFFENEN" SIND DEUTLICH AUFWENDIGER

Mit der DSGVO wird der innerbetriebliche Aufwand bei der Datenerhebung steigen, ebenso wie jener bei der Verwaltung oder Weitergabe von Daten. Das Recht auf Auskunft, Richtigstellung oder Löschung umfasst künftig auch die Auskunft über die Speicherdauer. Ein Unternehmen muss in der Lage sein, innerhalb eines Monats die geforderten Maßnahmen zu setzen. Kopfzerbrechen dürfte das nun niedergeschriebene "Recht auf Vergessen werden" bereiten: Demnach muss ein Unternehmen all jene, denen personenbezogene Daten übermittelt wurden, über eine allfällige Richtigstellung, Löschung oder Einschränkung der Datenverarbeitung informieren. Auch die "Datenmobilität" wird erheblichen Investitionsbedarf nach sich ziehen. Betroffene erhalten nämlich das Recht, Ihre Daten vom Auftraggeber herauszuverlangen, und zwar in einer "strukturierten Form" und in einem "üblichen, maschinenlesbaren Format". Der Betroffene kann sogar verlangen, dass ein Auftraggeber Daten direkt an einen anderen Auftraggeber überträgt.

DATENSCHUTZ NEU DENKEN

Angesichts des exponentiellen Wachstums an Datenmengen, die im Zuge der rasch fortschreitenden Digitalisierung entstehen, sowie der strengeren gesetzlichen Rahmenbedingungen ist es laut **DI Harald Leitenschüller, CTO, Microsoft Österreich**, schließlich an der Zeit, Datenschutz vollkommen neu zu denken. Unter dem Titel "Next Generation Privacy" wurde den Gästen ein Cloud-basiertes Konzept an Security- und Compliance-Maßnahmen vorgestellt, das ein hohes Maß an Transparenz und Kontrolle über die eigenen, personenbezogenen Daten eines jeden Anwenders ermöglicht. Indem Kunden selbst auf ihre Daten zugreifen und diese nach Wunsch löschen können, werden auch die Unternehmen, die ihre Daten verarbeiten und speichern, entlastet.

Mehr Eigenverantwortung für Unternehmen

Die DSGVO bringt eine Ausdehnung der Rechte von Betroffenen und verschärfte Sanktionen bei Verstößen. Unternehmen ("Verantwortliche" und "Auftragsverarbeiter") haben nach Inkrafttreten der Verordnung erweiterte Informationspflichten gegenüber "Betroffenen". Letztere haben das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und auf Herausgabe der Daten ("Datenmobilität"). Sie müssen jederzeit ihre Kontroll- und Dokumentationspflichten umfassend nachweisen können. Das bedeutet in der Praxis: Sie müssen ein Verzeichnis sämtlicher Verarbeitungstätigkeiten führen, einen Datenschutzbeauftragten einsetzen, für die Sicherheit der Datenverarbeitung sorgen, den zum Teil geänderten Melde- und Benachrichtigungspflichten nachkommen und unter Umständen eine Datenschutz-Folgeabschätzung treffen.

DIE TECHNIK MUSS STIMMEN

Fest steht, dass Unternehmen künftig deutlich stärker in die Pflicht genommen werden und es höchste Zeit ist, sich mit den rechtlichen Anforderungen und Pflichten auseinanderzusetzen. Dass hierfür die technische Komponente von essenzieller Bedeutung ist, erklärte **Rudolf Roschitz, Head of Business Development, S&T AG**. Was vielen Unternehmen nicht wissen oder zumindest nicht ausreichend im Blick haben, ist, dass beispielsweise die firmeneigenen Drucker eine der größten Schwachstellen sind, etwa dann, wenn Lohnzettel, Personal- und Krankenakte im Drucker liegen bleiben oder firmenfremde Geräte am Netzwerkanschluss des Druckers betrieben werden können. S&T unterstützt Kunden dabei, Problemfelder und Schwachstellen rasch zu identifizieren und ein adäquates und durchaus kosteneffizientes Lösungsdesign zu entwickeln. Schließlich kommt es im Zuge der DSGVO vor allem darauf an, Technik und Recht zu harmonisieren. Professionelle Dienstleister an seiner Seite zu haben, ist dabei unerlässlich. ■

 **Druckversion DSGVO: Die Uhr tickt immer lauter**