SEQIS: Die EU Datenschutz-Grundverordnung – Auswirkungen auf die IT

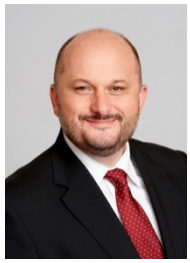
SEQIS, der führende österreichische Anbieter in den Spezialbereichen Software Test und IT Analyse, wird seiner Vorreiterrolle in der Branche wieder einmal gerecht und bereitet sich schon lange auf die neue EU Datenschutz-Grundverordnung (DSGVO) vor. Die SEQIS Experten erweiterten ihr Know-how hinsichtlich Datenschutz und Security und bieten ihre Unterstützung in diesen Bereichen an.

Mödling, 27.03.2018 – Bald ist sie da: Die EU(-weite) DSGVO tritt mit 25. Mai 2018 in Kraft. Die Dichte der Nachrichten und Artikel seit rund einem Jahr machen klar, dass sich wohl kein Unternehmen diesem Thema entziehen bzw. dieses ignorieren kann.

Vordergründig sind die Strafen bei Verletzungen deutlich angezogen worden – abhängig vom Vergehen bis zu 20 Mio. € bzw. 4% des konzernalen Umsatzes. Die bislang vergleichsweise geringen Strafen von bis zu 25.000 € haben den Aufwand für eine intensive Sicherung zumindest kalkulatorisch nicht gerechtfertigt – mit der neuen Verordnung kommt aber mehr Druck ins System und dies hat unmittelbare Auswirkung auf die IT Analyse und den Software Test.

Im Vergleich dazu sind bislang folgende Gesetze zum Datenschutz heranzuziehen: Das Datenschutzgesetz 2000 (DSG 2000) sowie speziellere, branchenspezifische Gesetze, wie zum Beispiel das Bankwesengesetz.

Schwerpunkte der DSGVO
War beim DSG 2000 der Schutz des Ausspionierens durch den Staat noch wesentlicher Schwerpunkt der Gestaltung, so wird bei der DSGVO den aktuellen Möglichkeiten und Trends mehr Rechnung getragen. Höheres Datenaufkommen durch z.B. IoT, Informationen über Mobilität durch GPS, Vernetzung von Daten durch Auswertungen und Analysen (BigData) bis hin zum Umgang in den Social Networks (Facebook und Co.).


Mag. Alexander Weichselberger, SEQIS Managing Partner
© SEQIS GmbH

„Wir werden bereits ausspioniert! Jetzt geht es (nur noch) darum, die personenbezogenen Daten zu schützen und die Selbstkontrolle über Daten zu verbessern. Auch Kindern soll durch die DSGVO ein besonderer Schutz eingeräumt werden“, so Mag. Alexander Weichselberger, Managing Partner bei SEQIS, zur Bedeutung der neuen Verordnung.

Personenbezogene Daten müssen besonders geschützt werden
Unter personenbezogene Daten fallen alle Informationen, die sich auf bereits identifizierte oder identifizierbare natürliche Personen beziehen (Anm: Juristische Personen sind – wahrscheinlich auch in Österreich – ausgenommen; allerdings wird aktuell der Bezug zwischen den Vertretern der juristischen Personen und deren schützenswerte Daten diskutiert; hier werden wohl auch noch Handlungsdirektiven kommen). Beispiele hierfür sind persönliche Daten wie Name, Anschrift, Geburtsdatum, religiöse oder politische Einstellung, Vorstrafen sowie körperlicher oder geistiger Gesundheitszustand.

SEQIS GmbH | Neusiedler Straße 36 | 2340 Mödling | Austria
T: +43 (0) 2236 320 320 0 | F: +43 (0) 2236 320 320 350
info@SEQIS.com | www.SEQIS.com
Firmenbuchnummer/commercial registry number: 204918a | UID/VAT: ATU51140607

„Identifizieren Sie deshalb Ihre Verarbeitungen mit personenbezogenen Daten und erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten. Stellen Sie sich die Frage: Welche personenbezogene Daten verantworten, verarbeiten und/oder übertragen Sie in welche Systeme? Berücksichtigen Sie auch unbedingt Systeme in der Cloud, die Sie eingebunden haben – und fragen Sie sich nach Datenverwendungen, die Sie selbst nicht hergestellt haben (Drittdatenquellen)! By-the-way: Ihre personenbezogenen Daten werden in Ihrem Unternehmen sicherlich auch als Excel-Auswertungen und Listen in den Filesystemen, in Email-Systemen, etc. vorkommen. Haben Sie diese Systeme schon auf Ihrer Liste? Hier noch eine Empfehlung: Damit Ihr Verzeichnis künftig aktuell bleibt, sollten Sie für Updates und Erweiterungen Ihrer Systeme Ihre Definition of Done bzw. Quality Gates entsprechend anpassen“, so Mag. Weichselberger weiter.

Erweiterte Pflichten bei der Datenverarbeitung
Mit der DSGVO wurden eine Menge Grundsätze verabschiedet, die große Herausforderungen mit sich bringen. Viele IT Lösungen müssen diese Anforderungen erst implementieren – falls das überhaupt (sinnvoll) möglich ist (Stichwort Legacysysteme). Darüber hinaus kommen auch neue Rollen und Verantwortlichkeiten ins Spiel – beide Punkte münden das Basisproblem der Zuständigkeit: Datenschutzbeauftragte mit IT Kenntnissen und noch mehr Analysten, Entwickler und Tester für die Aktualisierung – und dies vor dem Hintergrund der mangelhaften Verfügbarkeit von IT Spezialisten in der EU!

Ein weiteres Beispiel zu diesem Punkt: Unter „Integrität und Vertraulichkeit“ geht es um einen angemessenen Schutz durch geeignete technische und organisatorische Maßnahmen. Im Zusammenhang mit dem „Bericht Cyber Sicherheit 2017“ stellt sich die Frage: Wenn sich die Cyber-Kriminalität weiter so rasch entwickelt, neue Geschäftsmodelle wie „Ransomware-as-a-Service“ bzw. „Crime-as-a-Service“ angeboten werden und sogar Staaten sich selbst als Hacker engagieren – wie soll dann ein Unternehmen mit vergleichsweise bescheidenem Budget dagegen ankommen?

Die Antwort ist schlicht und einfach – alle Systeme müssen abgesichert werden:

- Erkennen & reagieren (IDS/IPS, SIEM)
- Kommunikation sichern (PKI, KMS)
- Erhalten & verbessern (SDLC, ISMS)

Wichtig sind dabei auch entsprechende Selbsttests. Besser, die Schwachstellen werden selbst erkannt, bevor es andere tun.

Natürlich sollte dies einem dem Risiko angemessenen und entsprechenden Schutzniveau dem angepassten Aufwand gegenüberstehen. Im Falle von Standardsoftware ist die Nachfrage beim Anbieter nach dem entsprechenden Update häufig ausreichend. Ist Individualsoftware in Verwendung, dann sollte rasch ein Updateauftrag für die Individualentwicklung vergeben werden.

Viele der neuen Grundsätze, wie z.B. „Recht auf Auskunft“, „Recht auf Vergessen werden“, „Recht auf Datenübertragung“ und das „Recht auf Beschränkung der Verarbeitung“ sollten auf Basis eines hohen Automatisierungsgrads entwickelt werden. Es geht darum, dass durch diese Services nicht zu viele Personen aus Ihrem Unternehmen gebunden werden!

SEQIS GmbH | Neusiedler Straße 36 | 2340 Mödling | Austria
T: +43 (0) 2236 320 320 0 | F: +43 (0) 2236 320 320 350
info@SEQIS.com | www.SEQIS.com
Firmenbuchnummer/commercial registry number: 204918a | UID/VAT: ATU51140607

Darüber hinaus wurden mit der DSGVO auch einige Fristen fixiert – im Regelfall wird eine Frist von einem Monat, bei entsprechender Komplexität bis zu 3 Monate, gewährt.

Wohin die Reise führt...
Mag. Weichselberger abschließend: „Zusammengefasst werden Sie sich in Richtung Datenschutz-Managementsystem (DS-MS) auf den Weg machen müssen.
Wesentliche Stützen dieses DS-MS sind Strategie und Reporting, Prävention sowie Operation und Fehlermanagement. Auch unterschiedliche Zertifizierungen und Datenschutzprüfzeichen sind am Markt bereits vorhanden. Diese Empfehlungen können Sie dabei unterstützen rechtzeitig und richtig auf die DSGVO vorbereitet zu sein. Hilfe gibt es darüber hinaus – wie immer – auch bei SEQIS."

Sie möchten mehr zum Thema DSGVO erfahren?
Auf der SEQIS Webseite finden Sie weitere Informationen:
www.SEQIS.com/de/blog/die-eu-datenschutz-grundverordnung
www.SEQIS.com/de/rueckblick-events-index

Kennen Sie schon den SEQIS Videoblog?
Hier finden Sie darüber hinaus wertvolle Tipps zur EU DSGVO: www.SEQIS.com/youtube

Über SEQIS
SEQIS ist der führende österreichische Anbieter in den Spezialbereichen Software Test und IT Analyse: Beratung, Verstärkung, Ausbildung und Workshops – seit 2001 der Partner für hochwertige IT-Qualitätssicherung. Weitere Informationen zum Unternehmen finden Sie unter www.SEQIS.com.

Für weitere Presseinformationen wenden Sie sich bitte an:
SEQIS GmbH
Marketing
Frau Julia Kremsl
Tel. +43 (0) 2236 320 320 0, marketing@SEQIS.com

Hinweis im Sinne des Gleichbehandlungsgesetzes:
Aus Gründen der leichteren Lesbarkeit wir in diesem Text die geschlechtsspezifische Differenzierung nicht durchgehend berücksichtigt. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

SEQIS GmbH | Neusiedler Straße 36 | 2340 Mödling | Austria
T: +43 (0) 2236 320 320 0 | F: +43 (0) 2236 320 320 350
info@SEQIS.com | www.SEQIS.com
Firmenbuchnummer/commercial registry number: 204918a | UID/VAT: ATU51140607