„10 things I wished they'd told me!"

aktuell. innovativ. praxisbezogen.

SEQIS

„10 things I wished they'd told me!"

Julia Kremsl, MA
Marketing

SEQIS

Darum SEQIS...

Foto: ©SEQIS Software Testing GmbH

SEQIS „10 things“ – Programm 2017

16.03.2017	Agile Testing Strategie für die effiziente Continuous Delivery von Microservices
01.06.2017	**Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test**
21.09.2017	Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse
16.11.2017	Sind Sie (sich) wirklich sicher? – IT Security im Fokus

Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test

Mag. Alexander Weichselberger
Geschäftsleitung

SEQIS

Disclaimer

10 things I wished they'd told me!

Bitte beachten Sie:

Die Informationen, Meinungen und Rechtsansichten in dieser Präsentation sind nicht als allgemein rechtsverbindliche Darstellung gedacht und können eine individuelle, auf die Besonderheiten des Sachverhaltes bezogene rechtliche Prüfung jedenfalls nicht ersetzen.

10 things
I wished they'd told me!


© Fotolia.com/adam121

10 things
I wished they'd told me!

https://www.dsb.gv.at

10 things
I wished they'd told me!

DSGVO
"one law, one continent"

Kinder: Besonderer Schutz

Natürliche Personen: Recht auf Schutz ihrer personenbezogener Daten wurde gestärkt

Selbstkontrolle über Daten

Personenbezogene (pb) Daten

- Namen, Anschrift, Geburtsdatum, Foto, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, religiöse oder politische Einstellung, rassische & ethnische Herkunft, Gewerkschaftszugehörigkeit, Urlaubsplanungen
- Persönliche Vorlieben und Verhalten, Arbeitsleistung und Beurteilungen, Zuverlässigkeit, sexuelle Vorlieben
- Informationen über (Vor)strafen, Strafdaten, Verurteilungen
- Einkommen, Kapitalvermögen, Schulden, Eigentum (Haus, Wohnung, Auto,…), Kreditkartendaten, Bankkonten
- Sozialversicherungsnummer, Personalnummer, Kfz-Kennzeichen, Kundennummer
- Informationen über körperliche & geistige Gesundheitszustand, genetische und biometrische Daten, Proben
- Aufenthaltsort oder Ortswechsel
- Online Kennungen: IP Adressen, Cookiekennungen, Mac Adressen
- Aufnahmen optoelektronischer Vorrichtungen.

10 things
I wished they'd told me!

1. **Identifizieren Sie die Verarbeitungen mit personenbezogener Daten**

Welche pb Daten verantworten, verarbeiten und/oder übertragen Sie in welchen Systemen?

Verzeichnis von Verarbeitungstätigkeiten

- Pflicht des Verantwortlichen & Auftragsverarbeiters
  - Firmen: 250+ Mitarbeiter ODER
  - Risiko für Rechte und Freiheiten der betroffene Personen ODER
  - Regelmäßige Verarbeitung (z.B. Lohnverrechnung, Kundenbetreuung) ODER
  - Sensible Daten bzw. Daten über strafrechtliche Verurteilungen werden verarbeitet

Verzeichnis von Verarbeitungstätigkeiten

- Inhalt / Aufbau
  - Namen & Kontaktdaten, Vertreters & Datenschutzbeauftragten
  - Zweck der Datenverarbeitung (Bestellsystem; Empfehlung: inkl. Rechtsgrundlage, z.B. Einwilligungserklärung)
  - Kategorien betroffener Personen, Daten sowie Empfängern (z.B. Kunden & Lieferanten; Rechnungsdaten, Adressdaten; Sozialversicherung, Finanzamt, Steuerberater & Konzernmutter USA)
  - Vorgesehenen Löschfristen der verschiedenen Datenkategorien
  - Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit)
  - Wenn Datenschutz – Folgeabschätzung notwendig
    - Sensible Daten, neue Technologie, hohes Risiko für Rechte & Freiheiten Betroffener,…

10 things
I wished they'd told me!

2. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten

Erweitern Sie Ihre DoD / Quality Gates (auch für Updates, Erweiterungen)

Generelles Verbot mit Erlaubnisvorbehalt

- Personenbezogene Daten dürfen nicht verarbeitet werden, außer: Betroffener willigt eindeutig ein
  - Zweckgebundene Einwilligung je Verarbeitung gesondert notwendig, nachweisbar
- Rund 40 Ausnahmen
  - u.a. Sicherheit & Verteidigung, Strafverfolgung, Behörden, persönliche /familiäre Angelegenheiten, überwiegendes berechtigtes Interesse des Verarbeiters, öffentliches Interesse, Computer-Notdienste (CERT, CSIRT)

CERT – Computer Emergency Response Teamwww.cert.at
CSIRT – Computer Security Incident Response Team http://www.csirt.org

EU Datenschutzgrundverordnung (DSGVO) Grundsätze

Grundsatz	Bedeutung	Herausforderungen
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Transparenz: Wer hat wann wie welche Daten bearbeitet / gespeichert / übermittelt / gesehen	• Applikationsübergreifende Zugriffsprotokollierung
Zweckbindung	Festgelegt und eindeutig („Dafür…“)	• Neue Features, neue Anwendungen – Prüfung: neuer Zweck (!)
Datenminimierung	Angemessen und auf notwendiges Maß beschränkt vs. Vorratsdatenspeicher	• Reduktion um (sensible) persönliche Daten
Richtigkeit	Sachlich richtig und erforderlichenfalls auf neuesten Stand	• Falsch? Löschen oder korrigieren • Übertragene Daten (Google.at → Google.com)
Speicherbegrenzung	Daten werden nur so lange gespeichert, wie erforderlich	• Löschung obligat, wenn nicht mehr notwendig • verteilte Applikationen + Übertragungen, Widersprüche
Integrität und Vertraulichkeit	Angemessener Schutz durch geeignete technische und organisatorische Maßnahmen	• Cyber Security • Minimalberechtigungen vs. DB Zugriff durch Applikationsowner, PW änderbar
Rechenschaftspflicht	Einhaltung der Grundsätze müssen nachweisbar sein	• Auditing

- „[… Bedrohungslage nach wie vor als ansteigend einzustufen.
- Neue Geschäftsmodelle
  - Randsomware-as-a-Service
  - Crime-as-a-Service
- Cyber Kriminalität hat sich rasch entwickelt.]“

© Cyber Sicherheit Steuerungsgruppe, Mai 2017

10 things
I wished they'd told me!

3. Sichern Sie Ihre Systeme ab

- Erkennen & reagieren (IDS/IPS, SIEM), Kommunikation sichern (PKI, KMS), erhalten & verbessern (SDLC, ISMS)
- Führen Sie Penetration Tests durch

10 things zur IT Security am 16.11.17

IDS/IPS – Intrusion Detection / Prevention System
SIEM – Security Information and Event Management
PKI – Public Key Infrastruktur
KMS – Key Management System
SDLC – Secure Development Life Cycle
ISMS – Information Security Management System

IT Analyse / Requirement Engineering

- Grundsätze:
  - „Recht auf Auskunft" – Transparente Information (Art 12 Abs. 1)
  - „Recht auf Vergessenwerden" – Löschung (EG66)
  - „Datenminimierung" & „Speicherbegrenzung" (Art 5 Abs. 1 Buchst. c/e)
- Weiters
  - Recht auf Datenübertragbarkeit: „Datenbereitstellung in strukturierter, gängiger, maschinenlesbarer Form" (Art 20 Abs. 1)
  - Technikgestaltung („data protection by design") und Voreinstellung („data protection by default") (EG78)
  - Methoden zur „Beschränkung der Verarbeitung" (EG67)

10 things
I wished they'd told me!

4. Analysieren Sie Änderungsbedarf bestehender Applikationen

- Updateauftrag Individual SW
- Rückfragen Standard SW Anbieter
- Prüfen von Reportinglösungen

Fristen

- Rechte „innerhalb eines Monats“ (EG59, Art. 12 Abs. 3)
  - Auskunft, Berichtigung und Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, automatisierte Entscheidungsfindung einschließlich Profiling
  - Komplexität, Situation ggf. +2 Monate

10 things
I wished they'd told me!

5. Entwickeln Sie Standardprozesse für Rechte Betroffener

- Inkl. Prozessbeschreibungen, Trigger, Kennzahlen und Messung
- Verproben Sie diese laufend (Releasetest)

Fristen

- Rechte „innerhalb eines Monats“ (EG59, Art. 12 Abs. 3)
  - Auskunft, Berichtigung und Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, automatisierte Entscheidungsfindung einschließlich Profiling
  - Komplexität, Situation ggf. +2 Monate
- Verletzung des Schutzes personenbezogener Daten („Data Breach“)
  - Unverzüglich, spätestens 72 h nach Bekanntwerden

Data Breach

- Physischen, materiellen oder immateriellen Schaden
  - Verlust der Kontrolle über pb Daten / Einschränkung Rechte
  - Diskriminierung
  - Identitätsdiebstahl oder -betrug
  - Verlust Vertraulichkeit, Berufsgeheimnis
  - … andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile
- Schrittweise informieren, wenn 72h gefährdet (EG85)
- Beschreibung (EG86)
  - Art der Verletzung
  - Empfehlungen zur Minderung nachteiliger Auswirkungen
  - Abstimmung mit Aufsichtsbehörde
- Abwehr weiterer Verletzungen einleiten

Beispiel Krisenplan

1. Vorbereitet sein
2. Erste h entscheiden (30 min)
3. Fakten töten Mythen
4. Transparenz: völlig
5. Wer spricht? Nur einer
6. 100% korrekte Aussagen
7. Sofort und durchgängig ansprechbar
8. Zugang zu Informationen kontrollieren
9. Interne Kommunikation
10. Mitgefühl zeigen

- … und den Krisenplan immer wieder testen
  - Kriterien / Vorgaben können sich ändern
  - Data Breach Potential laufend analysieren

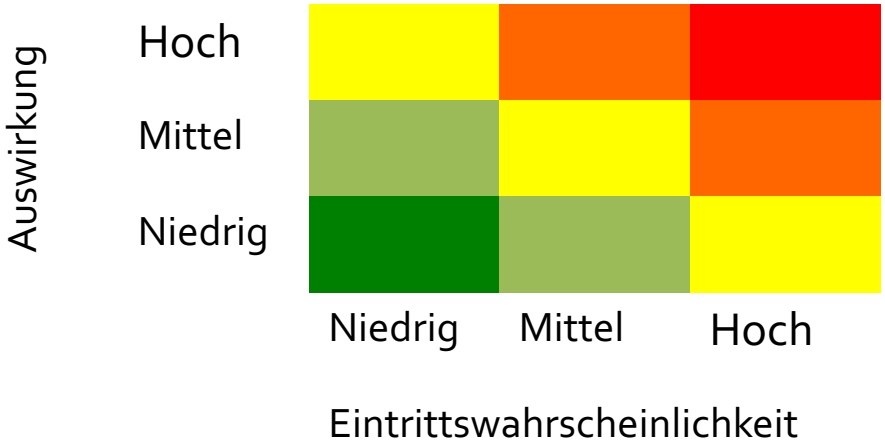
10 things
I wished they'd told me!

6. Erstellen und testen Sie Ihren Data Breach Krisenplan

Internes

- Dienstverträge aktualisieren („Geheimhaltung“, „Grundhaltung zum Datenschutz“)
  - Issuetracker, Logging
- Meldung von Leaks und Issues
  - Ordentlich bestätigen
  - Punkte einer Lösung zuführen
  - Risikobasierter Test

Risikostrategien



Datenschutzanforderungen haben einen höheren Verpflichtungsgrad wie alle Anforderungen an die IT-Sicherheit!

- Vermeidung (= Risikovermeidung)
  - Praxisnah?
- Behandlung (= Risikomodifikation) (Art 32)
  - Pseudonymisierung, Verschlüsselung (a)
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit sicherzustellen (b)
  - Wiederherstellung (c)
  - Audits (d)
- Transfer (= Risikoteilung)
  - Bußgeldbescheide nicht versicherbar
- Akzeptanz (= Risikobeibehaltung)
  - Eintrittswahrscheinlichkeit und Schadensersatz / Bußgeld wahrscheinlich

10 things
I wished they'd told me!

7. Bereiten Sie sich auch intern auf die neuen Regelungen vor

- Interne Datenschutz Vorschriften, Ausbildung & Prozesse
- Meldesystem für Issues und Leaks
- Wenige Basis-Risikostrategien

Anonymisierung & Pseudonymisierung

10 things
I wished they'd told me!

- Anonymisierung
  - Keine identifizierendes Datenfeld
    - 100% Anonymität bedeutet
      - Niemand im bekannten Universum kann
      - selbst mit unbeschränkt vielen Ressourcen (Computerleistung, Zusatzquellen)
      - heute und in Zukunft die betreffende Person identifizieren
  - \+ Anonymisierte Daten fallen nicht mehr in den Datenschutz
  - – Zumeist nicht viel wert (vgl. synthetische Daten)
    - Fehlernachstellen mit Datensalat? FK Constraints?

Anonymisierung & Pseudonymisierung

- Pseudonymisierung
  - „… die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“ (Art 4 Abs. 5)
  - Kurz: Name oder anderes Identifikationsmerkmal durch Pseudonym ersetzt; Ziel: Feststellung der Identität zu erschweren

Anonymisierung & Pseudonymisierung

DNA Studie: Medizinische Daten + PLZ / Geburtsdatum / Geschlecht	• Telefonbuchdaten
Netflix Pseudonym Kunde, Filmname + Verleihdatum	• IMDB Datenbank (Nickname, Filmname, Verleihdatum)
Freedom of Information Act (Transparenz von Behörden, z.B. NYC Taxi)	• Foto einer Person, die aus dem Taxi aussteigt (Strecke, Trinkgeld)
Smartphone	• GPS Daten + Zeit: Übernachtung? Lokale? Veranstaltungen? Einkauf? …

10 things
I wished they'd told me!

8. Berücksichtigen Sie die Grenzen der Anonymisierung und Pseudonymisierung

- Brauchbarkeit von wirklich anonymisierten Daten?
- Wie sicher sind Ihre pseudonymisierte Daten?

10 things
I wished they'd told me!

9. Prüfen Sie Ihre Auftragsverarbeiter

- Prüfung / Überarbeitung der DL-Verträge, Drittland-Check
- Haftung zu ungeteilter Hand (Geldbußen (Art. 83), Schadenersatz)

Projekt „Realisierung DSGVO“

10 things
I wished they'd told me!

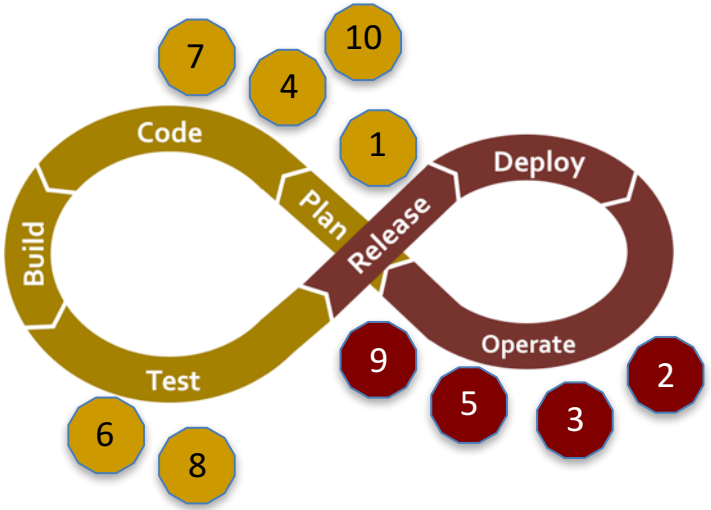
- Ziel: Datenschutzmanagement-System
  - Strategie & Reporting, Prävention, Operation & Fehlermanagement
- Durchgriff auf Ressourcen
  - Security/-test, Anforderungen, Vereinbarungen und Verträge,…
- Viele noch offen Anpassungen/Änderungen und Konkretisierungen → agil
- Zertifizierungen und Datenschutzsiegel/-prüfzeichen

10 things
I wished they'd told me!

10. Setzen Sie auf ein agiles DSGVO Projekt

Empfehlungen zur DSGVO

1. Identifizieren Sie die Verarbeitungen mit personenbezogener Daten
2. Erstellen Sie ein Verzeichnis zu Verarbeitungstätigkeiten
3. Sichern Sie Ihre Systeme
4. Analysieren und realisieren Sie Änderungsbedarfe Ihrer Applikationen
5. Entwickeln Sie Standardprozesse für Rechte Betroffener
6. Erstellen und testen Sie Ihren Data Breach Krisenplan
7. Bereiten Sie sich auch intern auf die neuen Regelungen vor
8. Berücksichtigen Sie die Grenzen der Anonymisierung und Pseudonymisierung
9. Prüfen Sie Ihre Auftragsverarbeiter
10. Setzen Sie auf ein agiles DSGVO Projekt



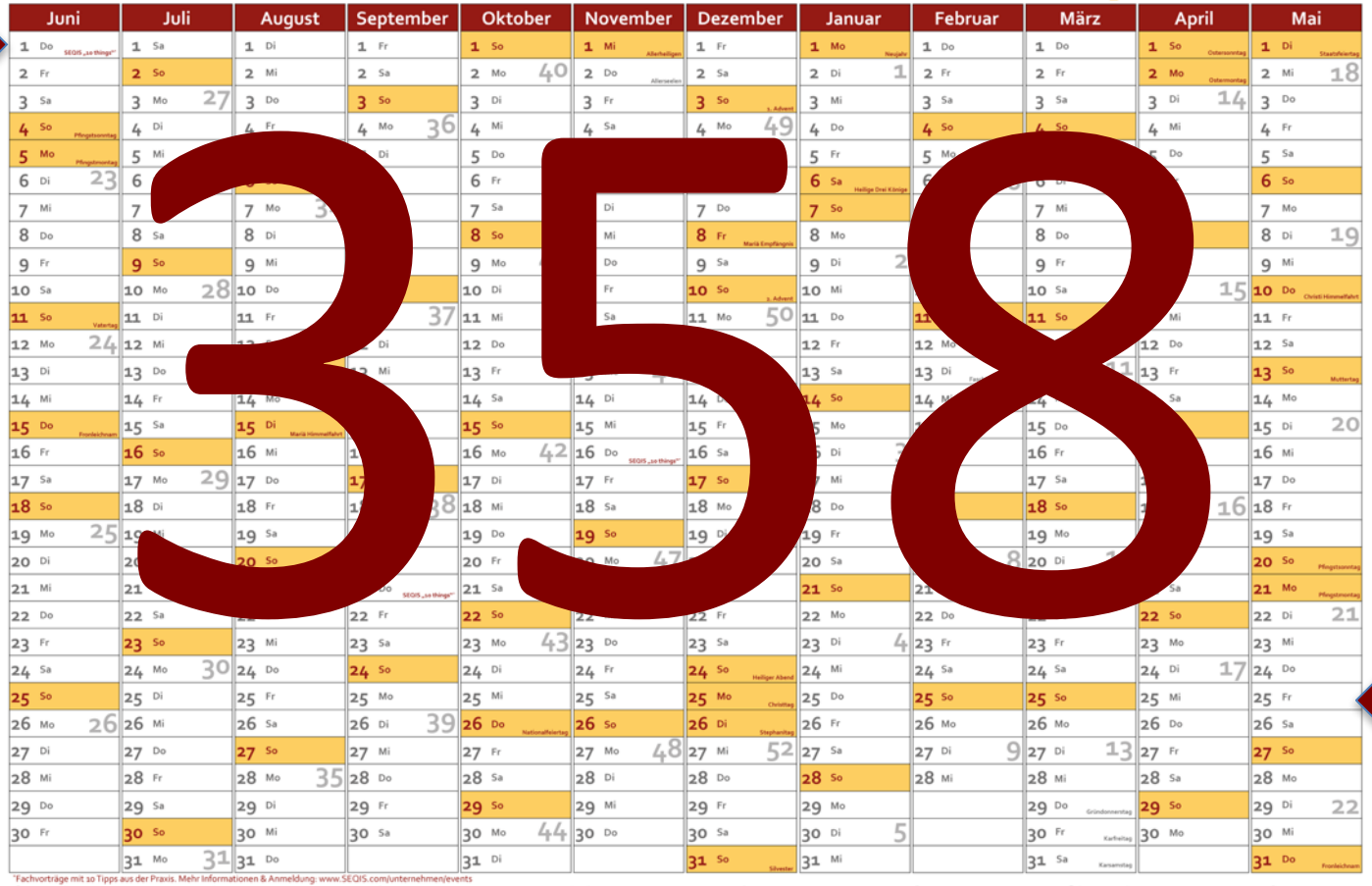
IT Analyse. Software Test. Better Results.

SEQIS 2017-18

... weil Softwarequalität wichtig ist! www.SEQIS.com 100% Analyse & Test

10 things wished they'd told me!

Heute



Juni	Juli	August	September	Oktober	November	Dezember	Januar	Februar	März	April	Mai
1 Do SEQIS „10 things"	1 Sa	1 Di	1 Fr	1 So	1 Mi Allerheiligen	1 Fr	1 Mo Neujahr	1 Do	1 Do	1 So Ostersonntag	1 Di Staatsfeiertag
2 Fr	2 So	2 Mi	2 Sa	2 Mo 40	2 Do Allerseelen	2 Sa	2 Di 1	2 Fr	2 Fr	2 Mo Ostermontag	2 Mi 18
3 Sa	3 Mo 27	3 Do	3 So	3 Di	3 Fr	3 So 1. Advent	3 Mi	3 Sa	3 Sa	3 Di 14	3 Do
4 So Pfingstsonntag	4 Di	4 Fr	4 Mo 36	4 Mi	4 Sa	4 Mo 49	4 Do	4 So	4 So	4 Mi	4 Fr
5 Mo Pfingstmontag	5 Mi	5 Sa	5 Di	5 Do			5 Fr	5 Mo		5 Do	5 Sa
6 Di 23	6			6 Fr			6 Sa Heilige Drei Könige				6 So
7 Mi	7	7 Mo 3		7 Sa	Di	7 Do	7 So				7 Mo
8 Do	8 Sa	8 Di		8 So	Mi	8 Fr Mariä Empfängnis	8 Mo				8 Di 19
9 Fr	9 So	9 Mi		9 Mo	Do	9 Sa	9 Di 2				9 Mi
10 Sa	10 Mo 28	10 Do		10 Di	Fr	10 So 2. Advent	10 Mi			15	10 Do Christi Himmelfahrt
11 So Vatertag	11 Di	11 Fr	37	11 Mi	Sa	11 Mo 50	11 Do			Mi	11 Fr
12 Mo 24	12 Mi		Di	12 Do			12 Fr			Do	12 Sa
13 Di	13 Do		Mi	13 Fr			13 Sa				13 So Muttertag
14 Mi	14 Fr			14 Sa	14 Di		14 So				14 Mo
15 Do Fronleichnam	15 Sa	15 Di Mariä Himmelfahrt		15 So	15 Mi	15 Fr					15 Di 20
16 Fr	16 So	16 Mi		16 Mo 42	16 Do SEQIS „10 things"	16 Sa					16 Mi
17 Sa	17 Mo 29	17 Do		17 Di	17 Fr	17 So					17 Do
18 So	18 Di	18 Fr		18 Mi	18 Sa	18 Mo					18 Fr
19 Mo 25		19 Sa		19 Do	19 So						19 Sa
		20 So		20 Fr	Mo 47						20 So Pfingstsonntag
			SEQIS „10 things"	21 Sa						Sa	21 Mo Pfingstmontag
22 Do	22 Sa		22 Fr	22 So		22 Fr	22 Mo	22 Do		22 So	22 Di 21
23 Fr	23 So	23 Mi	23 Sa	23 Mo 43	23 Do	23 Sa	23 Di 4	23 Fr	23 Fr	23 Mo	23 Mi
24 Sa	24 Mo 30	24 Do	24 So	24 Di	24 Fr	24 So Heiliger Abend	24 Mi	24 Sa	24 Sa	24 Di 17	24 Do
25 So	25 Di	25 Fr	25 Mo	25 Mi	25 Sa	25 Mo Christtag	25 Do	25 So	25 So	25 Mi	25 Fr
26 Mo 26	26 Mi	26 Sa	26 Di 39	26 Do Nationalfeiertag	26 So	26 Di Stephanitag	26 Fr	26 Mo	26 Mo	26 Do	26 Sa
27 Di	27 Do	27 So	27 Mi	27 Fr	27 Mo 48	27 Mi 52	27 Sa	27 Di 9	27 Di 13	27 Fr	27 So
28 Mi	28 Fr	28 Mo 35	28 Do	28 Sa	28 Di	28 Do	28 So	28 Mi	28 Mi	28 Sa	28 Mo
29 Do	29 Sa	29 Di	29 Fr	29 So	29 Mi	29 Fr	29 Mo		29 Do Gründonnerstag	29 So	29 Di 22
30 Fr	30 So	30 Mi	30 Sa	30 Mo 44	30 Do	30 Sa	30 Di 5		30 Fr Karfreitag	30 Mo	30 Mi
	31 Mo 31	31 Do		31 Di		31 So Silvester	31 Mi		31 Sa Karsamstag		31 Do Fronleichnam

25.5.18

*Fachvorträge mit 10 Tipps aus der Praxis. Mehr Informationen & Anmeldung: www.SEQIS.com/unternehmen/events

SEQIS Software Testing GmbH, Neusiedler Straße 36, 2340 Mödling, Austria · +43 (0)2236 / 320 320 - 0 · info@SEQIS.com · www.SEQIS.com · blog.SEQIS.com · facebook/SoftwareTestIsCool · twitter@SWTestIsCool

Quellen

- Datenschutzbehörde https://www.dsb.gv.at , 27.5.17
- Bericht „Cyber Sicherheit in Österreich 2017“ https://www.bka.gv.at/DocView.axd?CobId=66026, 29.5.17
- Datenschutz http://ec.europa.eu/justice/data-protection/article- 29/ documentation/opinion- recommendation/files/2014/ wp216_en.pdf

Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test

Mag. Alexander Weichselberger
Geschäftsleitung

SEQIS

SEQIS „10 things“ – Programm 2017

16.03.2017	Agile Testing Strategie für die effiziente Continuous Delivery von Microservices
01.06.2017	Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test
21.09.2017	Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse
16.11.2017	Sind Sie (sich) wirklich sicher? – IT Security im Fokus

„10 things I wished they'd told me!"

aktuell. innovativ. praxisbezogen.

SEQIS