„10 things I wished they'd told me!"

Die EU Datenschutz-Grundverordnung –

Auswirkungen auf den Test

10 Tipps & Tricks zum Nachlesen

SEQIS „10 things“

SEQIS, der führende österreichische Anbieter in den Bereichen Software Test und IT Analyse, gibt im Rahmen von kostenlosen Fachvorträgen rund um aktuelle Trendthemen 10 Tipps und Tricks zur Erfolgssteigerung in IT Projekten und praktischen Umsetzung im Arbeitsalltag.

Auf den folgenden Karten sind die 10 Tipps zum Thema „Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test“ übersichtlich zusammengefasst, sodass Sie diese jederzeit nachlesen können.

Einen ausführlichen Rückblick zur Veranstaltung sowie die Vortragsunterlagen zum Download finden Sie auf www.SEQIS.com/unternehmen/events

Vorwort EU Datenschutz-Grundverordnung

Durch die EU Datenschutz-Grundverordnung, kurz DSGVO, werden eine Vielzahl von Rechten und Pflichten für alle, die sich mit der Verarbeitung von personenbezogenen Daten beschäftigen, verpflichtend.

Insbesondere durch den hohen Strafrahmen, der, abhängig von den jeweiligen Vergehen, bis zu € 20 Mio. bzw. 4% des Konzernjahresumsatz ausmachen kann, macht der Gesetzgeber klar: Personenbezogene Daten gehören den Personen und damit muss man entsprechend sorgfältig umgehen.

Um diesem Aspekt Rechnung zu tragen und selbst DSVGO-fit zu werden, gilt es die richtigen Schritte zu tun und die verbleibende Zeit richtig zu nutzen. SEQIS verfügt über die entsprechenden Experten in den Bereichen Projektmanagement, IT Analyse und Software Test. Lassen Sie uns dieses Thema gemeinsam meistern!

Ihr

Alexander Weichselberger
SEQIS Geschäftsleitung

Disclaimer

Bitte beachten Sie:

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

1. Identifizieren Sie die Verarbeitungen mit personenbezogenen Daten

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

1. Identifizieren Sie die Verarbeitungen mit personenbezogenen Daten

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

Personenbezogene Daten, also alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, kommen in vielen IT Systemen vor: Datenbanken für CRM / ERP, Logistikanwendungen, Meldesystem für Behörden – aber auch in Filesystemen, in denen Sie z.B. Auswertungen von Kundenverhalten oder Namenslisten Ihrer Belegschaft führen. Auch Emailserver, die Sie ggf. nicht mal selbst betreiben und in denen Sie solche Listen an z.B. Ihre Unternehmensmutter in die USA verschicken („übertragen"). Cloudservices wie Dropbox und Co.? Ja, die gehören ebenfalls dazu!

Sammeln Sie in einem ersten Schritt alle Systeme, die am Datenfluss pb Daten beteiligt sind.

2. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten

Erweitern Sie Ihre DoD / Quality Gates (Updates, Erweiterungen), damit diese Verzeichnisse aktuell bleiben.

2. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten

Unternehmen mit 250+ MA sind verpflichtet, diese Verzeichnisse zu erstellen. Aber auch für andere, wenn Verarbeitungstätigkeiten mit Risiko für Rechte und Freiheiten Betroffener gemacht, die Verarbeitungen regelmäßig durchgeführt werden oder diese sensible Daten betreffen.

Inhalt / Aufbau:

- Namen & Kontaktdaten, Vertreter & Datenschutzbeauftragter
- Zweck der Datenverarbeitung (z.B. Bestellsystem; Empfehlung: inkl. Rechtsgrundlage, z.B. Einwilligungserklärung)
- Kategorien betroffener Personen, Daten sowie Empfänger (z.B. Kunden & Lieferanten; Rechnungsdaten, Adressdaten; Sozialversicherung, Finanzamt, Steuerberater & Konzernmutter in den USA)
- Vorgesehene Löschfristen der verschiedenen Datenkategorien
- Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen (nach Möglichkeit)
- Wenn Datenschutz – Folgeabschätzung notwendig: Kennzeichnung

3. Sichern Sie Ihre Systeme ab

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

Führen Sie Penetration Tests durch.

SEQIS „10 things" zur IT Security am 16.11.17

3. Sichern Sie Ihre Systeme ab

Sie müssen einen angemessenen Schutz durch geeignete technische und organisatorische Maßnahmen gewährleisten.

Das „Basisset" für sichere Systeme besteht aus folgenden Punkten:

- **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

Darüber hinaus sollten Sie zyklisch Pentration Tests durchführen – damit haben Sie ein klares Bild zu Ihrer persönlichen Cyber Sicherheit.

4. Analysieren und realisieren Sie Änderungsbedarfe Ihrer bestehenden Applikationen

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

4. Analysieren und realisieren Sie Änderungsbedarfe Ihrer bestehenden Applikationen

Durch die DSGVO werden den Betroffenen viele Rechte eingeräumt: Recht auf Auskunft, Löschung, Datenübertragbarkeit, usw. Und es wurden einige Grundsätze festgelegt: Datenminimierung, Speicherbegrenzung, Datenschutz durch Technikgestaltung („data protection by design“) und Voreinstellungen („data protection by default“).

Diese Anforderungen haben eines gemeinsam: Sie müssen einen hohen Automatisierungsgrad herstellen – sonst legen die Anfragen Ihr Unternehmen lahm. Damit müssen Sie Ihre bestehenden Applikationen aktualisieren: Ihre Individualentwicklungen müssen aktualisiert, Ihre Standard Software Lösungen wahrscheinlich updated und released werden.

Prüfen Sie bitte auch Ihre eigenen Reportinglösungen: Oftmals werden auch hier pb Daten verarbeitet und müssen verändert werden.

5. Entwickeln Sie Standardprozesse für Rechte Betroffener

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

5. Entwickeln Sie Standardprozesse für Rechte Betroffener

Mit der DSGVO wird auch die Erfüllungszeit für die Rechte der Betroffenen konkretisiert: Im Standard haben Sie 1 Monat Zeit die Anfragen und Wünsche zu erledigen – ist die Komplexität höher oder es erfordert die Situation, können Sie u.U. 2 Monate mehr bekommen.

Daher: Standardisieren Sie diese Prozesse, beschreiben, trainieren Sie sie. Legen Sie Kennzahlen (Reaktionszeiten, Durchlaufzeiten, etc.) fest und monitoren Sie diese.

Aus Testsicht sollten Sie diese Prozesse auch laufend verproben, insbesondere, wenn diese Rechte selten bis nie eingefordert werden.

Damit sind Sie fit für den Fall der Fälle.

6. Erstellen und testen Sie Ihren Data Breach Krisenplan

6. Erstellen und testen Sie Ihren Data Breach Krisenplan

Bei einem Data Breach („Datenpanne") ist die Sicherheit der von Ihnen verarbeiteten pb Daten nicht mehr gewährleistet. Für diesen Fall sollten Sie einen abgestimmten und etablierten (!) Krisenplan aus der Lade ziehen und mit der Schadensbegrenzung beginnen können.

Folgend beispielhaft der SEQIS-interne Plan für Krisen:

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) Interne Kommunikation
9) Zugang zu Informationen kontrollieren
10) Mitgefühl zeigen

Natürlich sollten Sie diesen Plan immer aktualisieren und testen!

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

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

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

Viele Maßnahmenempfehlungen richten sich prinzipiell nach außen (Betroffenenanfragen, Hacker, usw.). Aber wir wissen aus allen Securityuntersuchungen, dass die größten Probleme durch Fehlverhalten im Inneren ausgelöst werden. Daher:

- Prüfen Sie Ihre internen Vereinbarungen und Verträge: U.a. sollten Sie die Passagen zur „Geheimhaltung" und der „Grundhaltung zum Datenschutz" aktualisieren.
- Machen Sie in diesen Vereinbarungen klar, dass z.B. bei Issuetrackern und Logging möglichst keine pb Daten mit zu tracen sind.
- Etablieren Sie eine Kultur für die Meldung von Leads und Issues!

8. Berücksichtigen Sie die Grenzen der Anonymisierung und Pseudonymisierung

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

8. Berücksichtigen Sie die Grenzen der Anonymisierung und Pseudonymisierung

Anonymisierung und Pseudonymisierung erhöhen den Schutz pb Daten.

Dennoch sind anonymisierte Daten nicht für jeden Einsatzzweck geeignet – wie wollen Sie z.B. Fehler nachstellen, wenn Sie nicht konkret wissen, welche Daten verwendet wurden?

Auch die Pseudonymisierung ist kein Allheilmittel vor Leaks in den Daten: Durch hinzuziehen, insbesondere externer Datenquellen, können Rückschlüsse auf die natürlichen Personen oftmals hergestellt werden. Im Zusammenhang sollten Sie im Kontext auf k-Anonymität, l-Diversität und Verunreinigen von Daten als weitere Maßnahmen setzen.

Jedenfalls ist die Prüfung Ihrer diesbezüglichen Strategien ein wichtiger Test: Versuchen Sie einfach mal, Ihre pseudonymisierten Daten auf die Personen zurückzuführen. Ist interessant, macht Spaß und sichert Ihren Erfolg!

9. Prüfen Sie Ihre Auftragsverarbeiter

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

9. Prüfen Sie Ihre Auftragsverarbeiter

… Sie haben schon lange Rechenzentren, Cloudservices, Hosting und Big Data Datenanalysen externisiert? Diese Leistungen gehören nicht zu Ihren Kernkompetenzen? Passt – aber sichern Sie diese Datenverarbeitungen ab!

In der DSGVO wird eine Haftung zu ungeteilter Hand geregelt (Art. 83) – stellen Sie sicher, dass Ihre Sicherheitsstrategie auch mit den Auftragsverarbeitern abstimmt und getestet wird.

Beachten Sie auch, dass die Dienstleisterverträge aktualisiert werden und allfällige Forderungen aus der DSGVO berücksichtigt sind.

10. Setzen Sie auf ein agiles DSGVO Projekt

10. Setzen Sie auf ein agiles DSGVO Projekt

Für alle Aufgaben, die Sie im Zusammengang mit der DSGVO realisieren müssen, sollten Sie ein Projekt aufsetzen. Damit ist im Regelfall gewährleistet, dass Sie auf die notwendigen Ressourcen im Hause durchgreifen und die Änderungen rasch und zielorientiert umsetzen können.

Nachdem noch viele Fragen im Zusammenhang mit der DSGVO ungeklärt sind, werden auch noch Änderungen bis weit nach dem Stichtag 25.5.2018 auf uns zukommen. Daher sollten Sie einen agilen Projektansatz wählen.

Erwägen Sie auch Zertifizierungen: Damit kommen Empfehlungen und Richtlinien für die Realisierung der Anforderungen ins eigene Hause.

Zusammenfassung

1. Identifizieren Sie die Verarbeitungen mit personenbezogenen Daten
2. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten
3. Sichern Sie Ihre Systeme
4. Analysieren und realisieren Sie Änderungsbedarfe Ihrer bestehenden 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

Kontakt

© SEQIS Software Testing GmbH

Neusiedler Straße 36
A-2340 Mödling

Tel.: +43 2236 320 320 0
Fax: +43 2236 320 320 350

marketing@SEQIS.com
www.SEQIS.com

Folgen Sie uns:
blog.SEQIS.com
twitter.com/swtestiscool
facebook.com/SoftwareTestIsCool

Stand: Mai 2017