

Privacy trends 2011

Alfred Heiter

10. Juni 2011

ERNST & YOUNG
Quality In Everything We Do

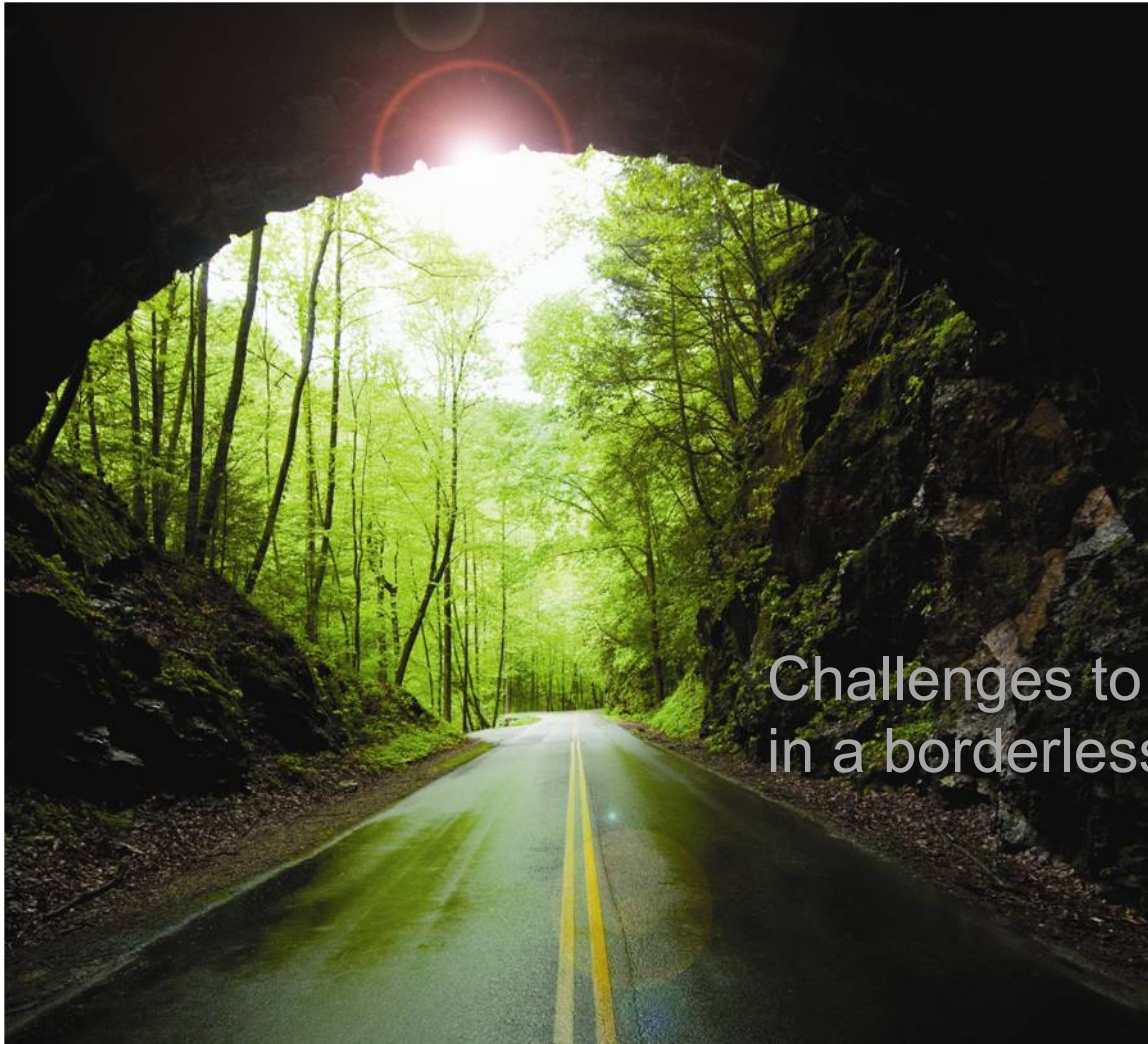
Vorstellung – Alfred Heiter



alfred.heiter@at.ey.com

- ▶ Seit 11 Jahren im IT-Prüfungs- und IT-Beratungsgeschäft
- ▶ Senior Manager bei Ernst & Young im Bereich Technology & Security Risks Services
- ▶ Schwerpunkte:
 - ▶ IT Governance, Risk and Compliance
 - ▶ IT Prüfung
 - ▶ IT Security
- ▶ Wirtschaftsprüfer, Steuerberater
- ▶ Certified Information Systems Auditor (CISA)
- ▶ Certified Information Systems Security Professional (CISSP)
- ▶ GIAC Certified Windows Security Administrator (GCWN)
- ▶ CGEIT Certified in the Governance of Enterprise IT
- ▶ Cobit Practitioner
- ▶ Mitglied ISACA Austria
- ▶ Mitglied des Fachsenats für Datenverarbeitung der Kammer der Wirtschaftstrehänder

Privacy Trends 2011



Challenges to privacy programs
in a borderless world

Gesetze, Regulierungen und deren Durchsetzung

- ▶ Änderung von früher zahnlosen Regelungen und Gesetzen
- ▶ US Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act)
 - ▶ Erweiterung der Befugnis von Staatsanwälten
- ▶ Update der EU Datenschutz-Richtlinie von 1995
 - ▶ Stärkung der Datenschutzbehörden, Verbesserung der Zusammenarbeit der Mitgliedsstaaten
 - ▶ Israels Datenschutzgesetze als „angemessenes Schutzniveau“ eingestuft
- ▶ Novellierung Datenschutzgesetz 2000 in Österreich in 2009
 - ▶ Videoüberwachung
 - ▶ Informationspflicht bei bekannter, unrechtmäßiger Verwendung



Kenntnis der aktuellen Gesetze und regelmäßige Überprüfung auf deren Einhaltung

Anforderungen an Meldungen von Vorfällen

- ▶ Nicht-Meldungen von Verstößen gegen den Datenschutz haben in der Vergangenheit zu Imageschäden geführt
- ▶ Ausgehend von USA wurden derartige Anforderungen weltweit gesetzlich verankert
 - ▶ HITECH Act (USA)
 - ▶ Personal Information Protection and Electronic Documents Act (PIPEDA) (Kanada)
 - ▶ Datenschutzrichtlinie, Telekom-Datenschutzrichtlinie (EU)
- ▶ Ursache von Verstößen
 - ▶ „Insider Threat“ durch mangelndes (Unrechts-) Bewußtsein
 - ▶ Awareness-Training und technische Kontrollen (z.B. Data Loss Prevention)



Entwicklung und Einführung eines Incident Response Plans
Einsatz von DLP Tools oder Services

Governance, Risk, Compliance Initiativen

- ▶ Investitionen in Government, Risk, Compliance (GRC) Initiativen wurden in den letzten Jahren intensiviert
- ▶ Markt für GRC Tools wächst
 - ▶ Spezialisierung auch auf Datenschutz-Management
- ▶ Trend zur Effizienzsteigerung der GRC Initiativen
 - ▶ Fokussierung auf wesentliche Risiken
 - ▶ Compliance Convergence
 - ▶ Datenschutz dabei weiterhin Top-Priority



Contiuous Monitoring im Bereich des Datenschutzes
Einsatz von GRC Lösungen, die auch Datenschutz berücksichtigen

Cloud Computing

- ▶ Vorteile von Cloud Computing: Kosten und Flexibilität
- ▶ Derzeit noch Vorbehalte seitens vieler Unternehmen wegen Risiken betreffend Datenschutz und Datensicherheit
- ▶ Verantwortlichkeiten der Unternehmen steigen
 - ▶ Lieferantenrisiko-Management
 - ▶ Cloud Services in unterschiedlichen geographischen Regionen mit unterschiedlichen Regelungen (z.B. PATRIOT Act in USA)
 - ▶ Informationen über Verstöße durch den Dienstleister
 - ▶ Aufbewahrungspflichten, Regelungen für Datenübermittlungen, Protokollierung von Zugriffen (der Cloud Administratoren), Zugriff durch Dritte



Ermittlung der notwendigen Prozesse und Daten
Gesetzliche oder vertragliche Regelungen (Einschränkungen)
Überwachung des Cloud Providers hinsichtlich Einhaltung der Vereinbarungen

Mobile Geräte

- ▶ Vermehrter Einsatz von Laptops, Mobiltelefone, Smart-Phones, Tablets
- ▶ Mobile Geräte → Mobile personenbezogene Daten
- ▶ Geo-Locating
 - ▶ Mitarbeiter: Transparente, klare Richtlinien
 - ▶ Kunden: Möglichkeit zur Zustimmung / Ablehnung
- ▶ Verschlüsselung
 - ▶ Teilweise vorgeschrieben
 - ▶ Schützt nicht vor Hacker / Cracker und Datenverlust
- ▶ Training der Benutzer



Einschätzung der Risiken von Geo-Locating
Verwendung angemessener Verschlüsselung
Überarbeitung der Datenschutzrichtlinien hinsichtlich mobiler Geräte

Soziale Netzwerke

- ▶ Internet, soziale Medien, Rund-um-die-Uhr Zugriff auf Informationen
- ▶ Informationen in sozialen Netzwerken
 - ▶ positive und negative Folgen
 - ▶ nicht leicht löschtbar („verewigt“), kein „Recht, vergessen zu werden“
- ▶ Datenschutzregelungen (Gesetze) adressieren die neuen Medien nur unzureichend
- ▶ Umgang mit sozialen Medien
 - ▶ Mitarbeiter: klare Richtlinien, wie soziale Netzwerke verwendet werden sollen, speziell auch im Bereich HR
 - ▶ Kunden: Kommunikation über den Umgang mit Informationen aus sozialen Netzwerken



Risiken und Herausforderungen von sozialen Netzwerke
Umgang mit Informationen von (potentiellen) Mitarbeitern
Training und klare Kommunikation von Richtlinien

Investitionen in Datensicherheit

- ▶ Investitionen in Datenschutz und Datensicherheit steigen wegen
 - ▶ Gesetzlicher / regulatorischer Anforderungen
 - ▶ Steigenden Risiken
- ▶ Überarbeitung der Governance Strukturen hinsichtlich Datenschutz und Datensicherheit
 - ▶ Datenschutzprogramme, aktualisierte Richtlinien, Awareness-Programme
 - ▶ Neu- und Wiederbesetzung von Positionen im Bereich GRC (z.B. Datenschutzbeauftragter)
 - ▶ Tools für Management von personenbezogenen Daten, Marken-Risikomanagement, internes Monitoring



Angemessene Budgetierung für Investitionen angesichts geänderter Risiko- und Complianceanforderungen
Notwendiges Personal für Datenschutz und Datensicherheit
Notwendige Tools für Überwachung der Verwendung von Daten

Evaluierung des Datenschutzes

- ▶ Fokus der internen Revision bisher breit gestreut
- ▶ Zukünftig stärkere Spezialisierung
 - ▶ Bereits jetzt Evaluierung der Kontrollen in Hinblick auf Data Leakage
 - ▶ Zukünftig verstärkter Fokus auf
 - ▶ Effektivität der Überwachung des Zugriffs auf personenbezogene Daten in Datenbanken und anderen Datenspeichern sowie im internen Netzwerk
 - ▶ Audits im Sinne von Beratung und Training
- ▶ Generally Accepted Privacy Principles (GAPP)
 - ▶ Entwickelt von AICPA und CICA
 - ▶ Rahmenwerk zur Entwicklung und Prüfung von Datenschutzprogrammen



Privacy Audits für 2011 planen
Training für interne Revisoren hinsichtlich Datenschutz-Risiken
Einsatz von GAPP für das Datenschutzprogramm

Reporting Standards für Dienstleistungsorganisationen

- ▶ Einfluss des IKS des Dienstleisters auf das IKS der outsourcenden Organisation
- ▶ Organisationen verlangen von Dienstleistern unabhängige Prüfung des IKS (im speziellen Datenschutz- und Datensicherheitsmaßnahmen)
- ▶ Prüfungsstandards: SSAE 16, ISAE 3402, IWP PE14 (neu)
- ▶ Guidance on service organization controls (SOC) reporting der AICPA im Entwicklung
 - ▶ Beschreibung der Datenschutzmaßnahmen des Dienstleisters
 - ▶ Bestätigung des Managements über Einhaltung der relevanten Gesetze und Standards sowie Effektivität des IKS
 - ▶ Beschreibung der durchgeführten Prüfungshandlungen und Bestätigung des Prüfers



Reports als Überwachung von Datenschutz und Datensicherheit
Beschreibung / Diskussion der erwarteten Datenschutzmaßnahmen

Privacy by Design

- ▶ Datenschutz bisher bei neuen Systemen und Lösungen erst im Nachhinein berücksichtigt
- ▶ Zukünftig ist Datenschutz wesentlicher Bestandteil des System Development Lifecycle (SDLC)
 - ▶ Privacy by Design Resolution (32nd International Conference of Data Protection and Privacy Commissioners)
 - ▶ Rolle der Datenschutzbeauftragten
 - ▶ Berücksichtigung von Datenschutz bereits in der Designphase



Einbettung von Datenschutz in den SDLC
Frühzeitige Einbindung des Datenschutzbeauftragten

Erwartungen des Datenschutzpersonals

- ▶ Umfangreichere Anforderungen und Aufgaben betreffend Datenschutz erfordern entsprechendes Personal
- ▶ Aufnahme von zusätzlichem, entsprechend qualifiziertem Personal
- ▶ Zusammenfassung von Funktionen zu GRC-Organisationen
 - ▶ HR
 - ▶ Recht
 - ▶ Datenschutz
 - ▶ etc.
- ▶ Datenschutz auch als Aufgabe für Funktionen / Positionen in anderen Bereichen
- ▶ Zertifizierungen (z.B. Certified Information Privacy Professional, CIPP)



Positionen, die über Datenschutzkenntnisse verfügen sollen
Zertifizierungen für Mitarbeiter, die mit personenbezogenen Daten
arbeiten

Zusammenfassung

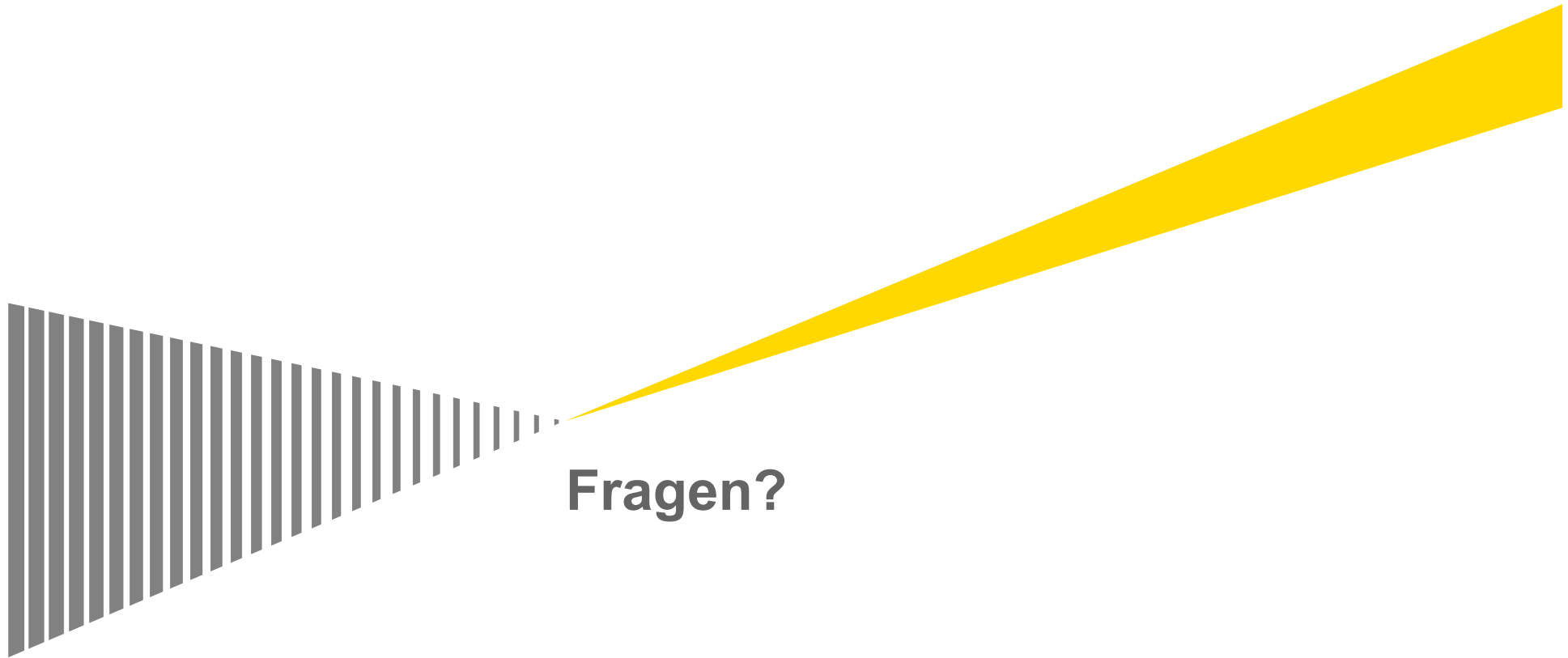
- ▶ Das räumlich klar abgegrenzte Arbeitsumfeld verändert sich durch mobile Kommunikation, soziale Netzwerke und Cloud Computing signifikant
- ▶ Neue Risiken für Organisationen und Mitarbeiter in Hinblick auf Datenschutz
- ▶ Gesetzgeber reagieren mit neuen Regelungen
 - ▶ Erleichterung des Informationsflusses
 - ▶ Strengere Kontrollen
- ▶ Investitionen in Datenschutzmaßnahmen
 - ▶ Einstellung von qualifizierten Personal oder Ausbildung bestehender Mitarbeiter
 - ▶ Verbesserung der Prozesse und Richtlinien
 - ▶ Verwendung von Tools

- ▶ Proaktiver Datenschutz

Ausblick

- ▶ Studie „Privacy trends 2011“ verfügbar im Internet
 - ▶ <http://www.ey.com/GL/en/Services/Advisory>

- ▶ Kontakt:
 - ▶ Alfred Heiter
 - ▶ +43 1 21170 1030
 - ▶ alfred.heiter@at.ey.com



Fragen?