Ergebnisse der EY Studien zu Datenschutz und Datendiebstahl

Gottfried Tonweber

EY
Building a better working world

Studie zum Reifegrad des Datenschutz-Managements in österreichischen Unternehmen

Eckpunkte der Studie

Teilnehmer

- 30 Studienteilnehmer aus 14 Branchen
- Größtenteils international operierende Unternehmen mit Hauptsitz in Österreich
- 19 der 30 Studienteilnehmer haben mehr als 500 Mitarbeiter
- Über 70 Prozent der befragten Unternehmen haben mehr als 70.000 Kunden

Studiendesign & Methodik

- Erhebungszeitraum von Mitte bis Ende 2016
- Erhebung erfolgte anhand eines standardisierten Fragebogens den Dimensionen Prozessen, Policies, Organisation und Legal
- 50 offene und geschlossene Fragen (davon 26 Kernfragen) aus sieben Kategorien (Allgemeines, Rechtlicher Rahmen, Datenschutzorganisation, Prozesse im Datenschutzmanagement, Datenverarbeitung, Datenschutzkommunikation und Risiken)
- Bewertung der geschlossenen Fragen mittels fünf-stufiger Bewertungsskala von „Stimme nicht zu“ bis „Stimme zu“ und der Option „Nicht zutreffend“

Limitationen der Studie

- Die Studie basiert nur auf Aussagen der Teilnehmer, nicht auf verifizierten Ergebnissen oder Effektivitätsprüfungen
- Alle Ergebnisse müssen zum Geschäftsmodell, zu Art und Größe des Unternehmens und insbesondere zu den vorhandenen Risiken in Relation gesetzt werden. Ein schlechtes Teilergebnis bedeutet nicht automatisch Handlungsbedarf, und ein gutes Ergebnis heißt nicht zwingend, dass alles zum Besten steht
- Insbesondere wurde nicht der Status der Datenschutz Compliance im Unternehmen untersucht, sondern die Umsetzung beziehungsweise der Reifegrad von Prozessen und Methoden zum Datenschutzmanagement

Auszug aus der Studie zum Thema Datenschutz in Österreich

EY DS Studie 2016/2017

75%

¾ der Befragten sagen: Datenschutz ist dem Top-Management sehr wichtig.
„Tone from the top“ passt!

75%

Bei ¾ der befragten Unternehmen beschäftigt sich nur bis zu maximal 1 Person mit Datenschutz

80%

80% der Befragten stehen nicht genügend finanzielle/personelle Ressourcen zur Verfügung;
¼ hat nicht einmal ein Budget für DS

Auszug aus der Studie zum Thema Datenschutz in Österreich

EY DS Studie 2016/2017

58% 58% haben keinen Datenschutzbeauftragten

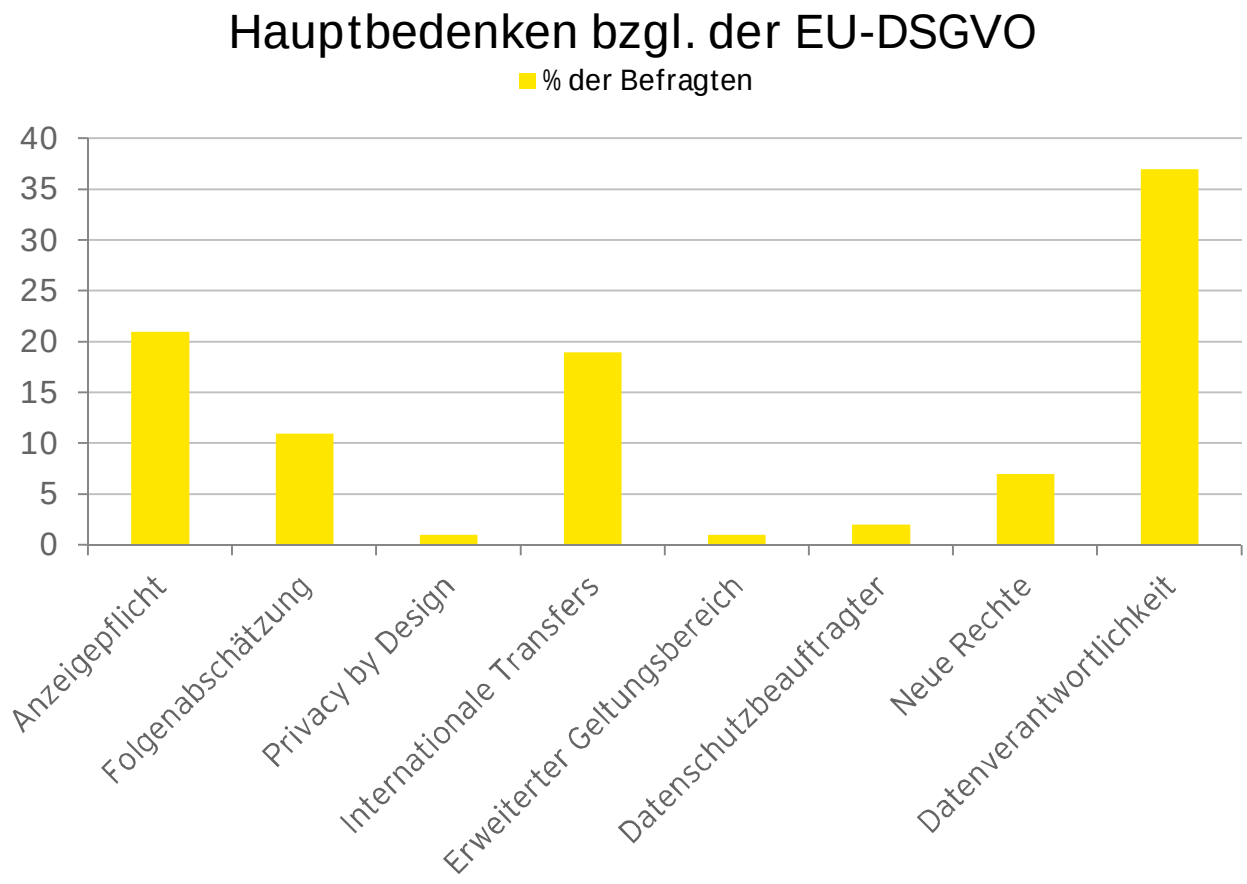
50% 50 % der befragten Studienteilnehmer lassen personenbezogene Daten von externen Servicedienstleistern verarbeiten.

44% Knapp die Hälfte der befragten Unternehmen hat noch keine internen Vorgaben (Policy) bezüglich Datenschutz

63% 63 % haben erforderliche Datenschutzprozesse, wie den Prozess zur Verständigung von Stakeholder im Falle eines „Privacy Breach“, noch nicht implementiert

Was unsere Kunden am meisten verunsichert?

Im Januar 2016[1)], haben wir 150 Klienten befragt, was Sie am meisten an der EU-DSGVO beunruhigt.



Top 3 Bedenken:

1. Datenverant-wortlichkeit
2. Obligatorische Anzeigepflicht
3. Datenüber-tragung

1) EY London event for European Data Protection Days on 28 January 2016

Datendiebstahl

Datendiebstahl

13.02.2013, 15:01

Jeder 2. Mitarbeiter nimmt Firmendaten bei Jobwechsel mit

Angestellte stehlen Daten und sind sich dabei keiner Schuld bewusst. Das ist das Ergebnis einer weltweiten Studie des Sicherheitsanbieters Symantec, der zufolge die Hälfte aller Mitarbeiter, die in den letzten zwölf Monaten ih haben, vertraulic davon gaben an, zu wollen.

ZDNet / Data & Storage

Anonymous hackt Kundendaten der österreichischen GEZ

Die Behörde bestritt den Datenverlust zunächst. Als Anonymous mit Veröffentlichung drohte, gestand sie ihn jedoch ein. Die Daten befanden sich

96.000

Datendiebstahl mit gefälschter Bank Austria-Nachricht

Gepostet am 04.05.2015 um 14:48 Uhr von **Watchlist Internet**
Themen: Phishing, Bank, Datenklau, E-Mail, Fälschungen

Kriminelle versenden eine gefälschte Bank Austria-E-Mail mit dem Betreff: „Kreditkarte zu Ihrem eigenen Schutz gesperrt". Darin fordern sie dazu auf, die Kreditkarte zu bestätigen und freizuschalten. Das soll auf einer externen Website getan werden.

ZEITREISE WISSEN RECHT MEINUNG MEH

UNTERNEHMEN UND

Datendiebstahl: Mitarbeiter gefährlicher als Cyberkriminelle

Datenleck bei Wiener Linien – 20.000 Kunden betroffen

Wiener-Linien-Kundendaten wurden bei einem externen Dienstleister entwendet.

WEB UND TECH

Erste Klage gegen Yahoo nach Diebstahl von 500 Mio. Kundendaten

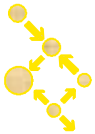
Der US-Konzern hatte den Datendiebstahl am Donnerstag bekanntgemacht und erklärt, er gehe auf Angriffe aus dem Jahr 2014 zurück.

Datendiebstahl in Österreich
EY-Studie

44% Fast jedes zweite Unternehmen in Österreich ist in den vergangenen Jahren Opfer von Spionage oder Datendiebstahl geworden, 30% sogar mehrfach

17% Jedes sechste Unternehmen in Österreich wurde bereits Opfer von Erpressungsversuchen

36% Jedes dritte Unternehmen wurden bereits Opfer durch Social Engineering



13.000 In Österreich gab es alleine 2016 über 13.000 Anzeigen wegen Cyberkriminalität

Anforderung an Unternehmen

75% Rund drei von vier Angriffen kommen durch das interne Kontrollsystem ans Licht (Studie EY, 2017)

Durch die EU-DSGVO gewinnt die Accountability des Unternehmens deutlich mehr an Gewicht

Die EU-DSGVO enthält die explizite Forderung, die Datenschutz Compliance zu gewährleisten und nachweisen zu können

Unternehmen haften, wenn keine ausreichende Sicherheitsmaßnahmen ergriffen wurden

EY-Vorgehensmodell

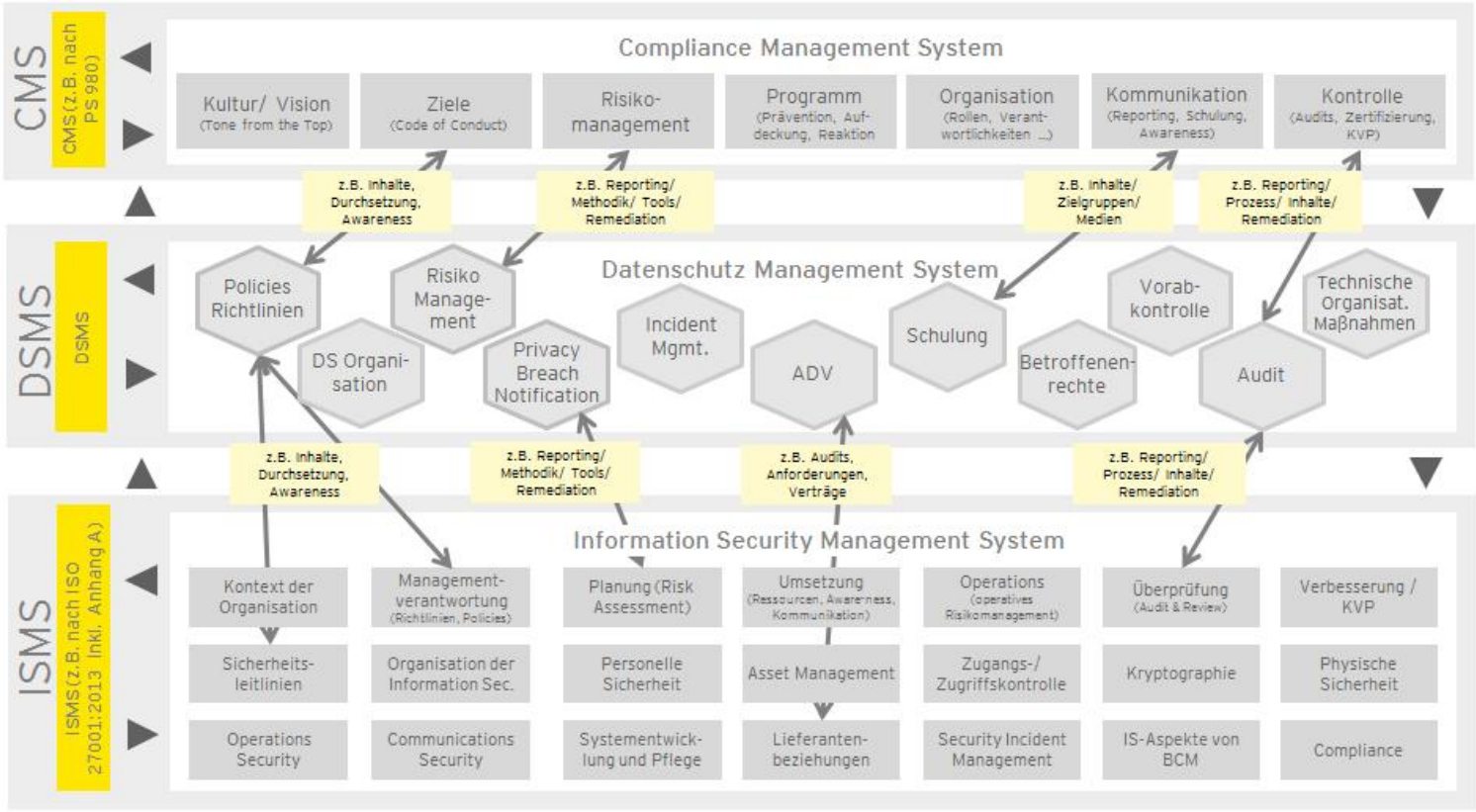
Unser Vorgehensmodell
Strukturiertes Datenschutzmanagement angelehnt an IDW PS 980

- Datenschutzmanagement kann sowohl bei der Implementierungsphase als auch bei der Einhaltung der Anforderungen einen wesentlichen Nutzen stiften
- Elemente eines strukturiertes Datenschutzmanagement basierend auf IDW PS 980:

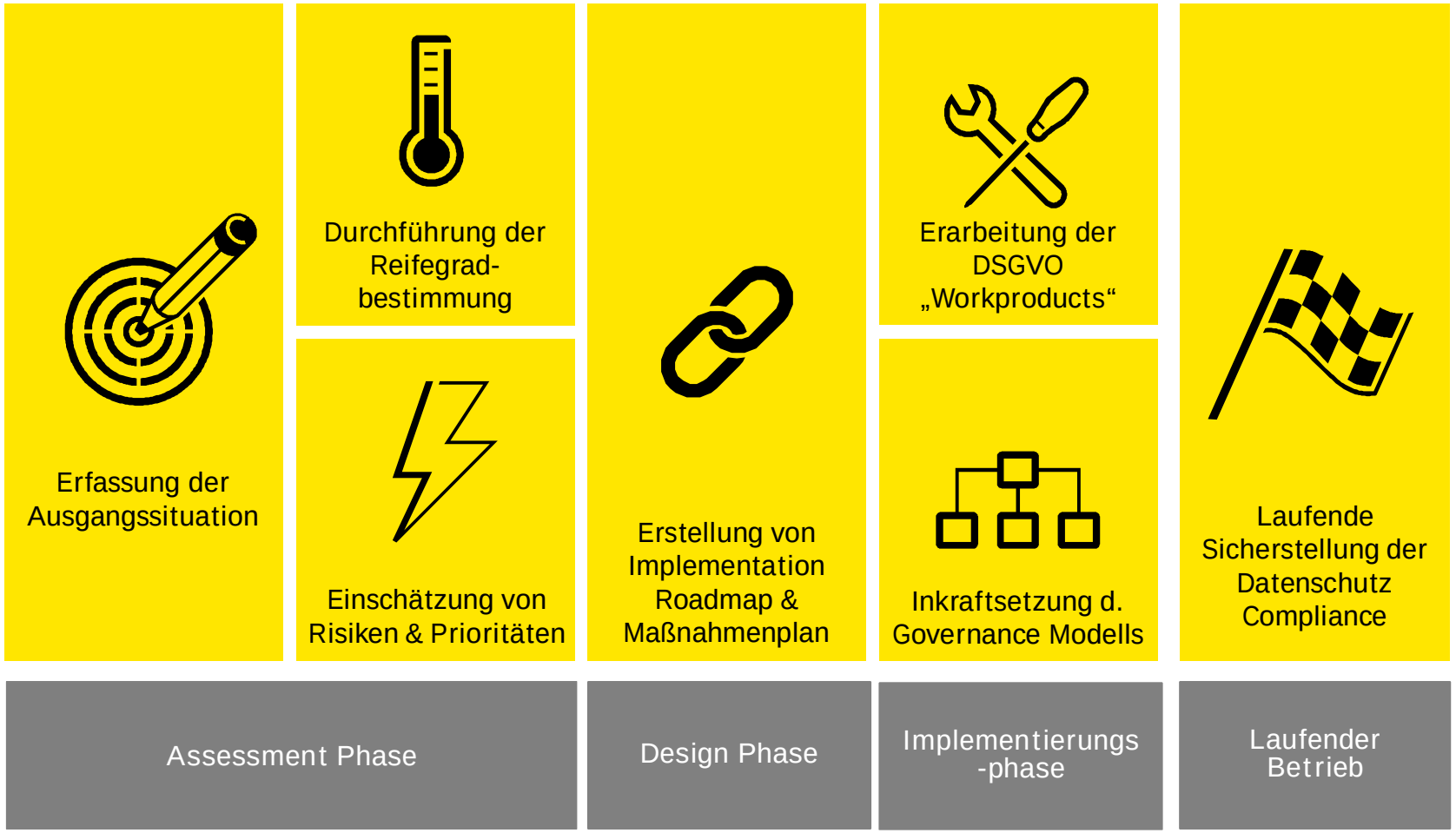
„Ein Datenschutz-managementsystem stellt die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen dar, mit denen der datenschutzkonforme Umgang mit personenbezogenen Daten im Unternehmen systematisch gemanaged wird."

Was ist das Ziel der Reifegradbestimmung?
Integration von Managementsystemen

- Einbindungsmöglichkeit eines Datenschutzmanagementsystems um Synergiemöglichkeiten optimal zu nutzen



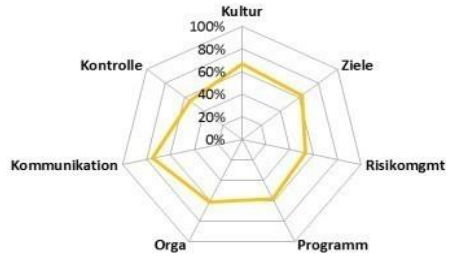
Bausteine zur Umsetzung und Aufrechterhaltung der DSGVO Compliance



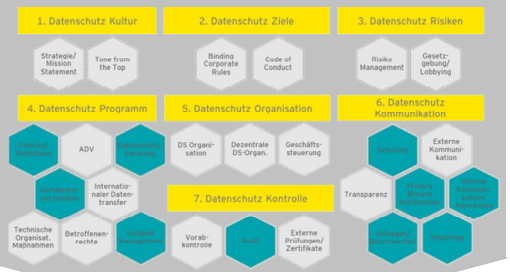
Was passiert mit den Ergebnissen der Interviews und der Reifegradbestimmung?
Erarbeitung eines Risikobasierten Maßnahmenplans

- Basierend auf den Ergebnissen der vorab durchgeführten Interviews, werden im Rahmen der nächsten Phasen Handlungsfelder identifiziert.
- Diese werden einer risikobasierten Einschätzung unterzogen und priorisiert.
- Darauf aufbauend erfolgt das Design der „DSGVO Workproducts“ und einer Implementation Roadmap.
- Diese dient als Basis für den nachfolgenden detaillierten Projektplan zur Maßnahmenumsetzung.
- Die in den Interviews erhobenen Informationen werden genutzt, um bereits parallel die Erstellung des Verfahrensverzeichnisses voranzutreiben.

Ergebnisse der IST-Erfassung

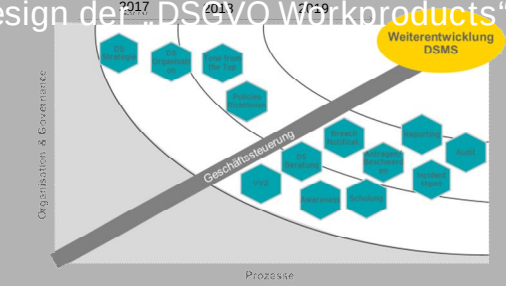


Risikoeinschätzung d. Handlungsfelder & Priorisierung notwendiger Maßnahmen

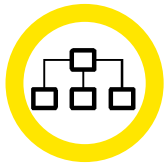


Detaillierter Projektplan für Maßnahmenumsetzung 2017 & 2018

Entwicklung d. Impl. Roadmap & Design der „DSGVO Workproducts“



Die „DSGVO Workproducts“ zur Gewährleistung einer kontinuierlichen Datenschutz Compliance



Definierte Rollen & Verantwortlichkeiten (Governance Modell)

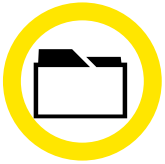
Verfahrens-verzeichnis

Datenschutzfolgen-abschätzung (DSFA)

Technische & Organisatorische Maßnahmen

Data Breach Notification Plan

Geregelter (internationaler) Datentransfer



Gesteuerte Archivierung & Löschung

Privacy by Design/ Default

Testing/Audit Plan

Aktualisierte Verträge & Betriebs-vereinbarungen

Prozesse zur Wahrung der Betroffenenrechte

Arbeitnehmer-information / Awarenessbildung

Kontaktinformationen

Gottfried Tonweber

Office: + 43 (1) 211 70 1145
Mobil: + 43 (664) 60003 1145
E-Mail: gottfried.tonweber@at.ey.com

Senior Manager und Leiter der Cyber Security Services bei EY Österreich. Mehr als 10 Jahre Erfahrung in IT Beratung und Prüfung in Österreich, Europa und weltweit.