DSGVO Compliance 2018

KPMG Security Services GmbH
Porzellangasse 51
1090 Vienna

Wien, Juni 2017

Ausgangslage „DSGVO“

Cybercrime in Österreich

KRIMINALSTATISTIK

Anstieg bei Cybercrime und Gewaltdelikten: 3,8 Prozent mehr Strafanzeigen im Vorjahr

Cybercrime in Österreich: Alle Branchen und Größenordnungen betroffen

Österreichs Unternehmen hinken in der IT-Sicherheit hinterher

26. Mai 2017, 10:50

posten

Ausgaben für den Schutz gegen Cyberkriminelle werden international oft als Investition und Chance gesehen

Wien – Weltweit stocken Unternehmen ihre Ausgaben für IT-Sicherheit auf, "in Österreich ist dieses Bewusstsein jedoch noch weniger stark ausgeprägt", schließt das Beratungsunternehmen PwC aus einer aktuellen weltweiten Umfrage. "Heimische Unternehmen hinken hier eindeutig nach" heißt es. International würden Ausgaben für den Schutz gegen Cyberkriminelle inzwischen oft als Investition und Chance gesehen.

futurezone Netzpolitik B2B Produkte Digital Life Science Meinung Games Apps Start-ups Community

Neue EU-Datenschutzregeln: Firmen läuft die Zeit davon

FIREBALL

Gefährliche Adware infiziert über 250 Millionen Computer

Die Adware Fireball hat ihren Ursprung in China. Sie manipuliert den Browser, spioniert User aus und kann nach Belieben Malware auf dem Rechner installieren.

IT-SICHERHEIT

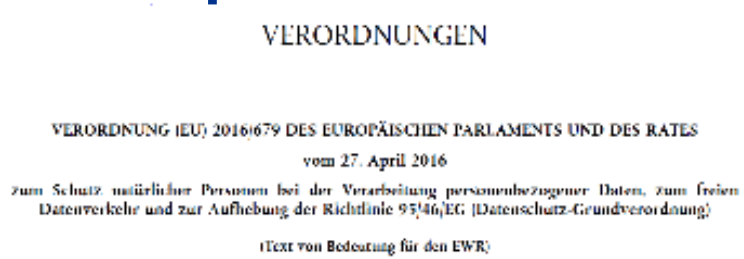
Nordkoreanische Hacker nahmen Nationalbank und Raiffeisen ins Visier

231 Postings

Sicherheitsforscher fanden im Code einer Schadsoftware eine Liste an Zielen, von denen Nordkorea Geld stehlen wollte

Ausgangslage „DSGVO“

Datenschutzgrundverordnung: Einheitliches Datenschutzniveau in Europa



VERORDNUNGEN

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

Ziel der Datenschutzgrundverordnung war die Herstellung eines einheitlichen Datenschutzniveaus in der EU

- Direkte Anwendung der DSGVO in jedem EU Mitgliedsstaat
- Teilweise noch nationaler Umsetzungsspielraum (Öffnungsklauseln)
- EU-weite Harmonisierung (Kooperations- & Kohärenzmechanismus)

25.05.2018

Inkrafttreten der DSGVO

Ausgangslage „DSGVO“

Die DSGVO stellt eine Reihe an neuen Anforderungen an Steuerberater

Privacy by design and default (Art 25)

— Setzung geeigneter technischer & organisatorischer Maßnahmen

1

Dokumentation von Verarbeitungsvorgängen (Art 30)

— Führen eines Verzeichnisses aller Verarbeitungstätigkeiten

2

Meldung von Datenschutz-verstößen (Art 33 ff)

— Unverzügliche Meldung an Aufsichtsbehörde (72h)

3

Datenschutz-Folgeabschätzung (Art 35 ff)

— Durchführung einer Risiko-abschätzung bei Verarbeitung von personenbezogenen Daten

4

Bestellung Datenschutz-beauftragter (Art 37 ff)

— Keine allgemeine Pflicht: Umsetzungsspielraum in nationalem Recht

5

Folgen bei Verstößen

— Stärkung der Rechtsbehelfe der Betroffenen (Art 77 ff)

— Anordnungsverfügung (Art 58)

— Geldbußen (Art 83)

6

Weiter Kernanforderungen (Auszug)

Einwilligung (Art 7)

— Eindeutige bestätigende Handlung zum Zeichen des Einverständnisses mit der Verarbeitung

1

Informationspflichten (Art 13)

— Nennung des Verantwortlichen

— Datenschutzbeauftragter

— Zweck der Verarbeitung

2

Recht auf Löschung und Einschränkung der Verarbeitung (Art 17ff)

— Right to be forgotten

— Limitierung der Verarbeitung nach Ende der rechtmäßigen Verarbeitungsdauer

3

Datenübertragbarkeit (Art 20)

— Auswahl der Datenverarbeitung und Übertrag der Daten an alternative Daten-Verarbeiter

4

Sicherheit der Verarbeitung (Art 32)

— Vertraulichkeit, Integrität, Verfügbarkeit und Belast-barkeit der Systeme zur Verarbeitung

5

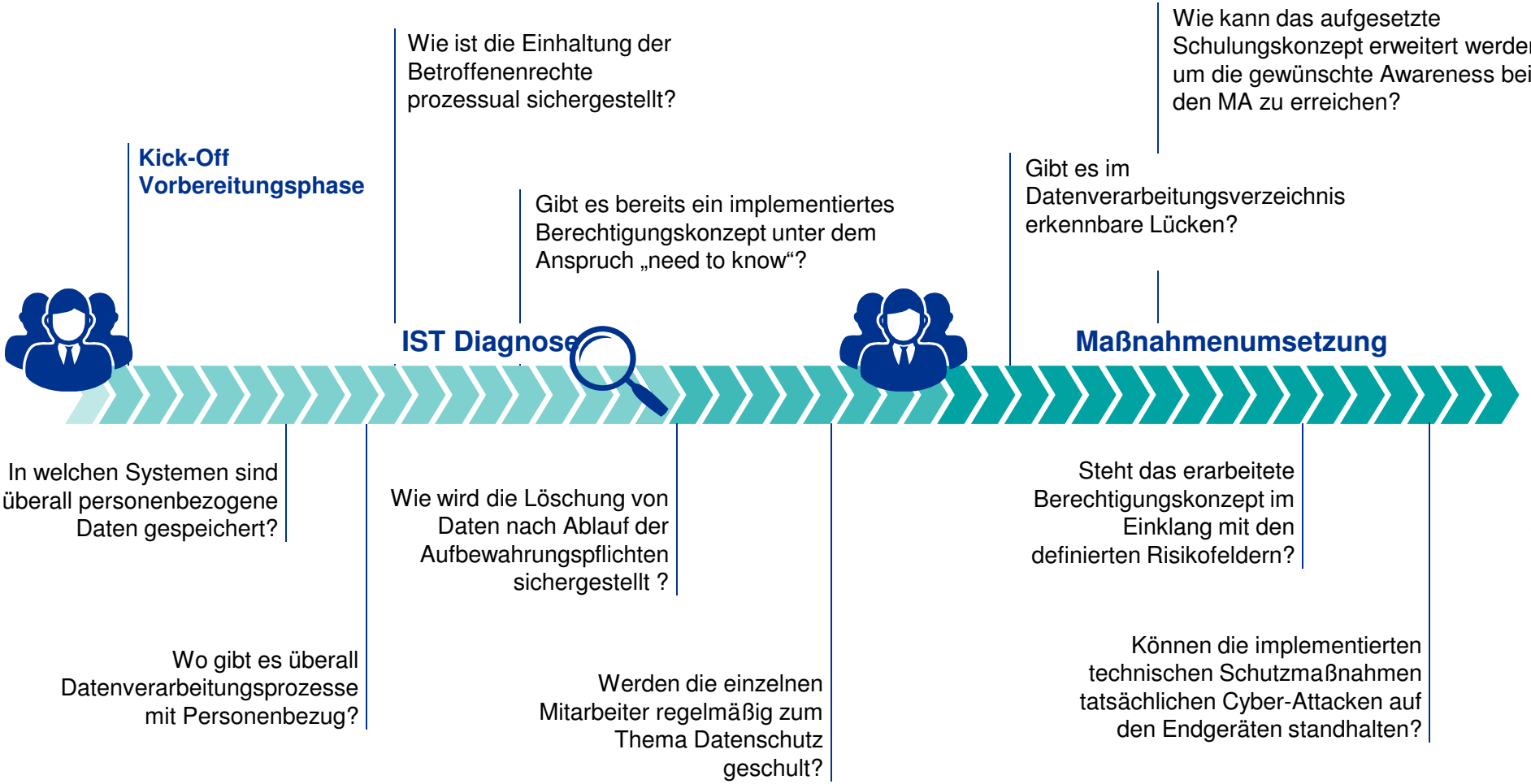
Verhaltensregeln (Art 40ff)

— Schaffung individueller Verhaltensregeln auf nationaler / Sektor Ebene z.B. Handel & Logistik

— Zertifizierung des Datenschutzniveaus (Art 40)

6

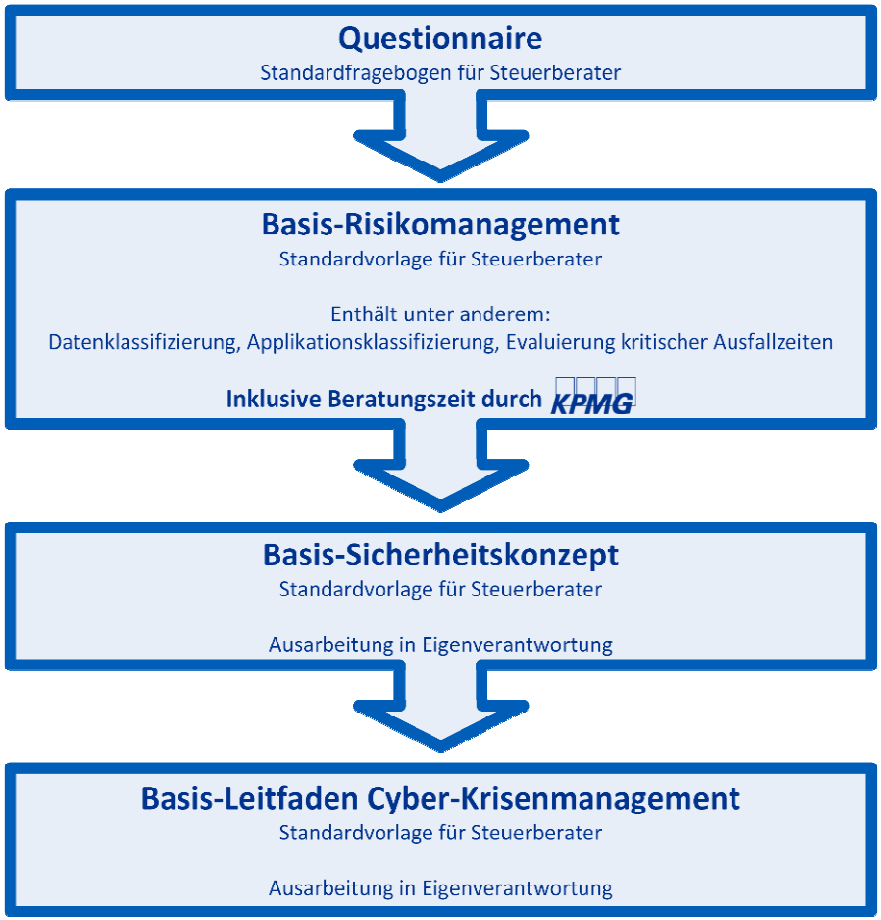
Fragen, auf die im Rahmen der DSGVO Umsetzung Antworten gefunden werden müssen



Matrix: DSGVO Anforderung vs RACI mit KPMG & DVO

	R Durchführung	A Rechenschaftspflichtig	C Konsultiert	I Informiert
Privacy by design and default	dvo + Steuer-berater	Steuerberater	Steuerberater	
Dokumentation von Verarbeitungsvorgängen	dvo + Steuer-berater	Steuerberater	KPMG	
Meldung von Datenschutz-verstößen	dvo KPMG	Steuerberater	KPMG	
Datenschutz-Folgeabschätzung	KPMG	Steuerberater	Steuerberater	dvo
Bestellung Datenschutz-beauftragter	KPMG	Steuerberater	Steuerberater	
Einwilligung	Steuerberater	Steuerberater		
Informationspflichten Zweck der Verarbeitung	Steuerberater	Steuerberater	Steuerberater	
Datenübertragbarkeit	dvo	Steuerberater	Steuerberater	
Sicherheit der Verarbeitung	dvo + Steuer-berater	Steuerberater	Steuerberater	

Das DSGVO-Grundlagenpaket für Steuerberater

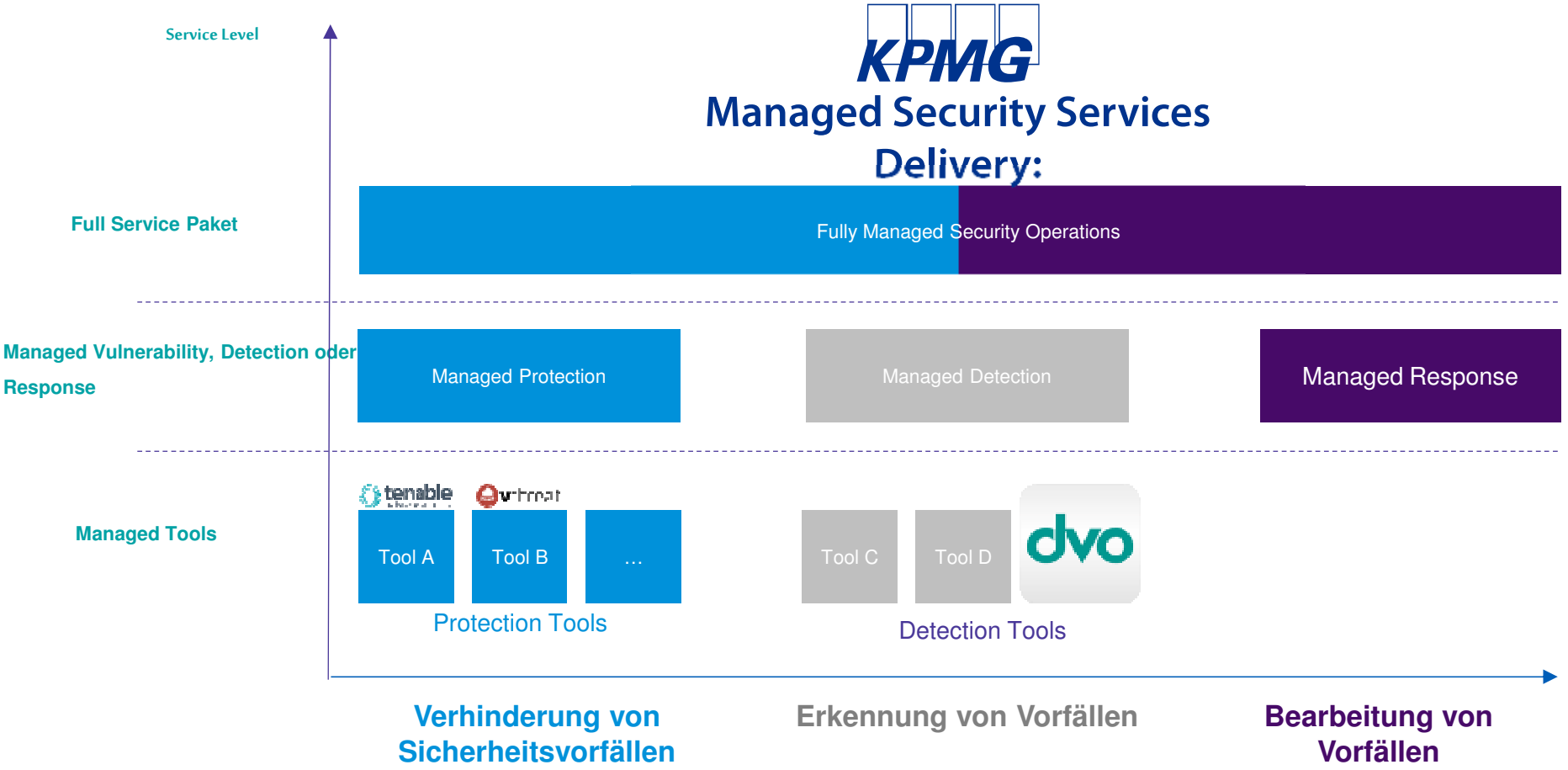


Eine Kooperation von KPMG + dvo

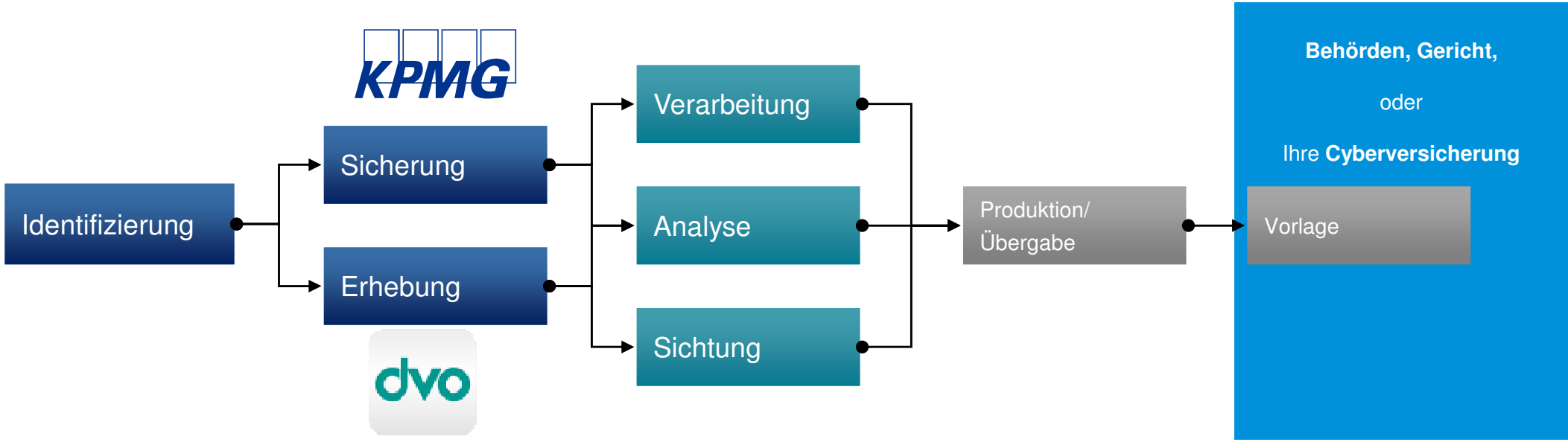
Erhältlich ab September 2017 bei dvo

DSGVO Ready

Wir unterstützen Sie im sicheren Betrieb



Beweissicherung im Schadensfall: Vorgehensweise



Fünf Prozessschritte:

Identifizierung: Feststellen aller vorhandener und relevanter Daten

Sicherung & Erhebung: Sämtliche, in Schritt eins identifizierte und relevante Daten werden gesichert

Verarbeitung: Alle Daten werden in einem speziellen Programm verarbeitet und können danach gesichtet und analysiert werden

Produktion/Übergabe: Alle relevanten Ergebnisse werden zusammengefasst

Vorlage: Die Ergebnisse können vor Gericht vorgelegt werden.

Datenschutzbeauftragte: Typische Aufgaben

Durch die Einführung der DSGVO gehen ergeben sich für die Datenschutzbeauftragen Eingangs eine Reihe von Einmalaufgaben, bevor ab Anfang 2018 mit einer Überführung in den Regelbetrieb zu rechnen ist.

2017: Einmalaufgaben zur Umsetzung der DSGVO

- ✓ Abstimmung mit lokalen Rechtsvorschriften.
- ✓ Definition und roll-out eines lokalen internen Privacy Statements/Briefings an regionale Mitarbeiter & Kunden
- ✓ Definition eines Audit Plans und Durchführungsanweisungen auf Basis der etablierten DSGVO Kontrollen.

Überführung in Regelbetrieb ab 2018

Wiederkehrende Tätigkeiten zur laufenden Compliance

- ✓ **Prüfung und Koordination von Datenschutzanfragen**
- ✓ **Durchführung von Datenschutzfolgeabschätzungen (Privacy Impact Assessments)**
- ✓ **Regelmäßige Prüfung des Verfahrensverzeichnis**
- ✓ **Behandlung von Data Breaches**, inklusive Unterstützung bei der Benachrichtigung der Betroffenen
- ✓ Laufendes Monitoring der Compliance, basierend auf den etablierten Kontrollen
- ✓ Unterrichtung zu geltenden Rechtsvorschriften
- ✓ Jährliche Erstellung eines DSGVO Status Reports
- ✓ Planung & Durchführung von Datenschutz Awareness Trainings
- ✓ Laufendes Monitoring der regionalen Gesetzgebung zur DSGVO Umsetzung und verwandter Regularien.

KPMG

Datenschutz @ KPMG

Führend bei Fragen zu Sicherheit und Datenschutz

WARUM KPMG?

#1

Forrester Research bewertet KPMG als Global Leader in der Cyber Security - Beratung

1500

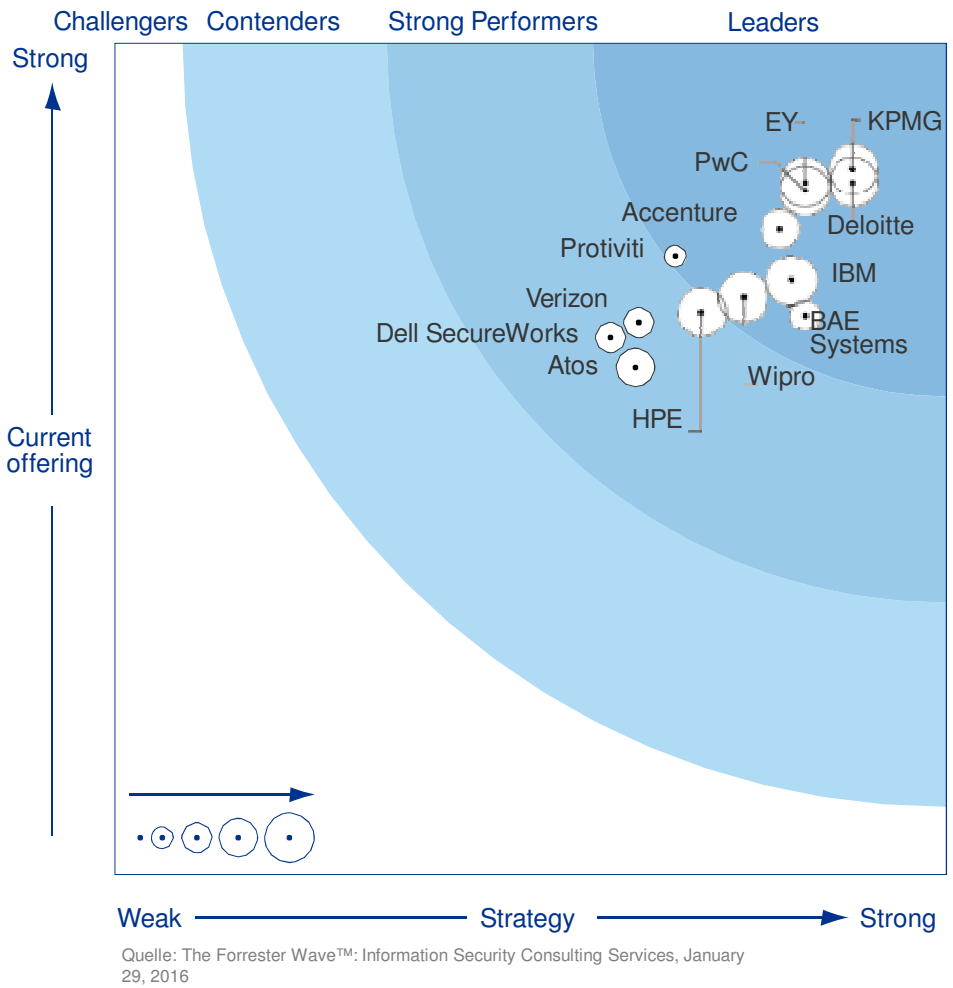
Globales Netzwerk aus 1500 Spezialisten für IT-Sicherheit

>20

Mehr als 20 Jahre Erfahrung im Bereich Applikations- und IT-Sicherheit

>100

In den letzten Jahren hunderte Projekte in den Bereichen IT-Sicherheit, Secure SDLC und Penetrationstests



Quelle: The Forrester Wave™: Information Security Consulting Services, January 29, 2016

KPMG

KPMG Cyber Security – global für Sie da!

Eine weltweite Präsenz

Unsere global agierende Cyber Security Einheit ist in allen wichtigen Regionen der Welt vertreten – in 29 Ländern insgesamt.

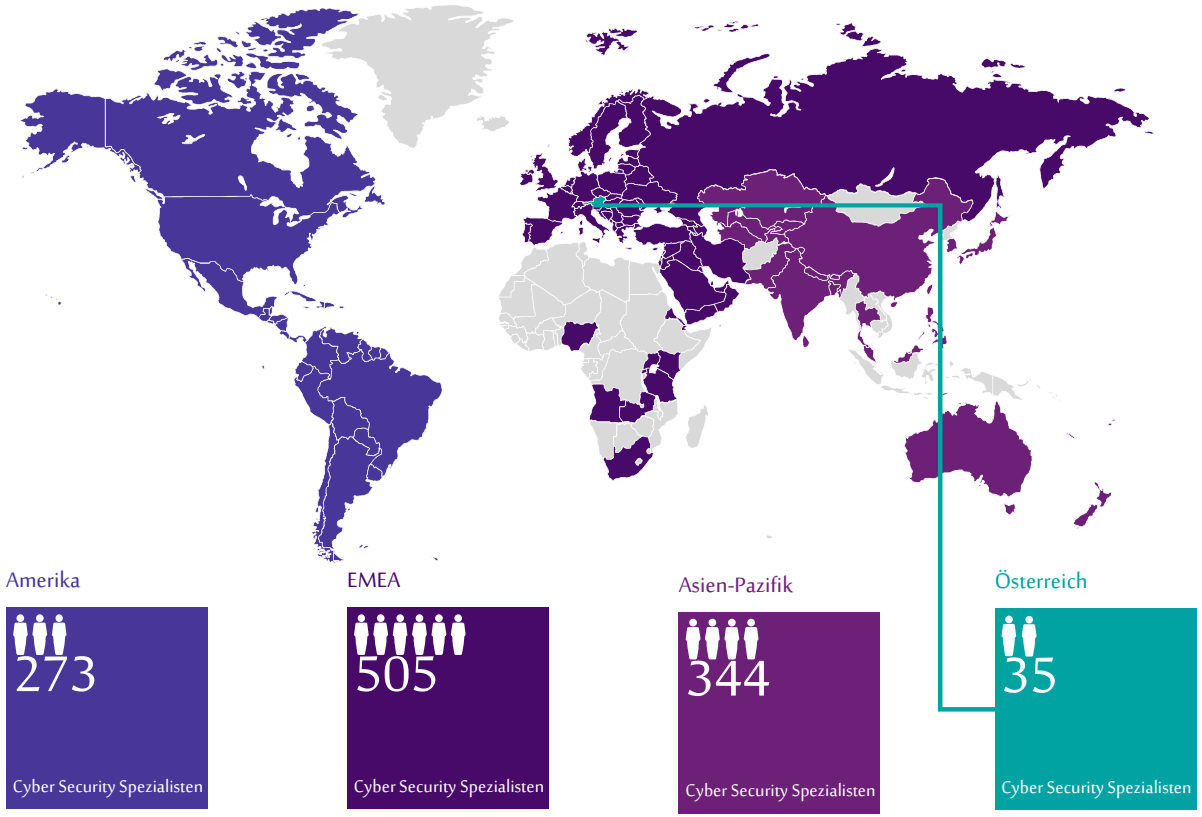
Ein erfahrenes Team

Wir investieren stark in die Aus- und Weiterbildung. Unsere eigene Cyber Academy gewährleistet, dass unsere Mitarbeiter am Ball bleiben. Wir verstehen, wie wichtig es ist, gut ausgebildete Spezialisten zu haben, weshalb wir die kontinuierliche Fortbildung unserer Mitarbeiter fördern.

Weltweit Spezialisten

Unser Cyber Security Team umfasst mehr als 1500 Cyber Security Spezialisten. Alle Spezialisten im Bereich der Informationssicherheit sind zB nach CISSP, CISM, OSCP qualifiziert sowie Mitglied im jeweiligen Berufsverband.

Globales Netzwerk an Niederlassungen

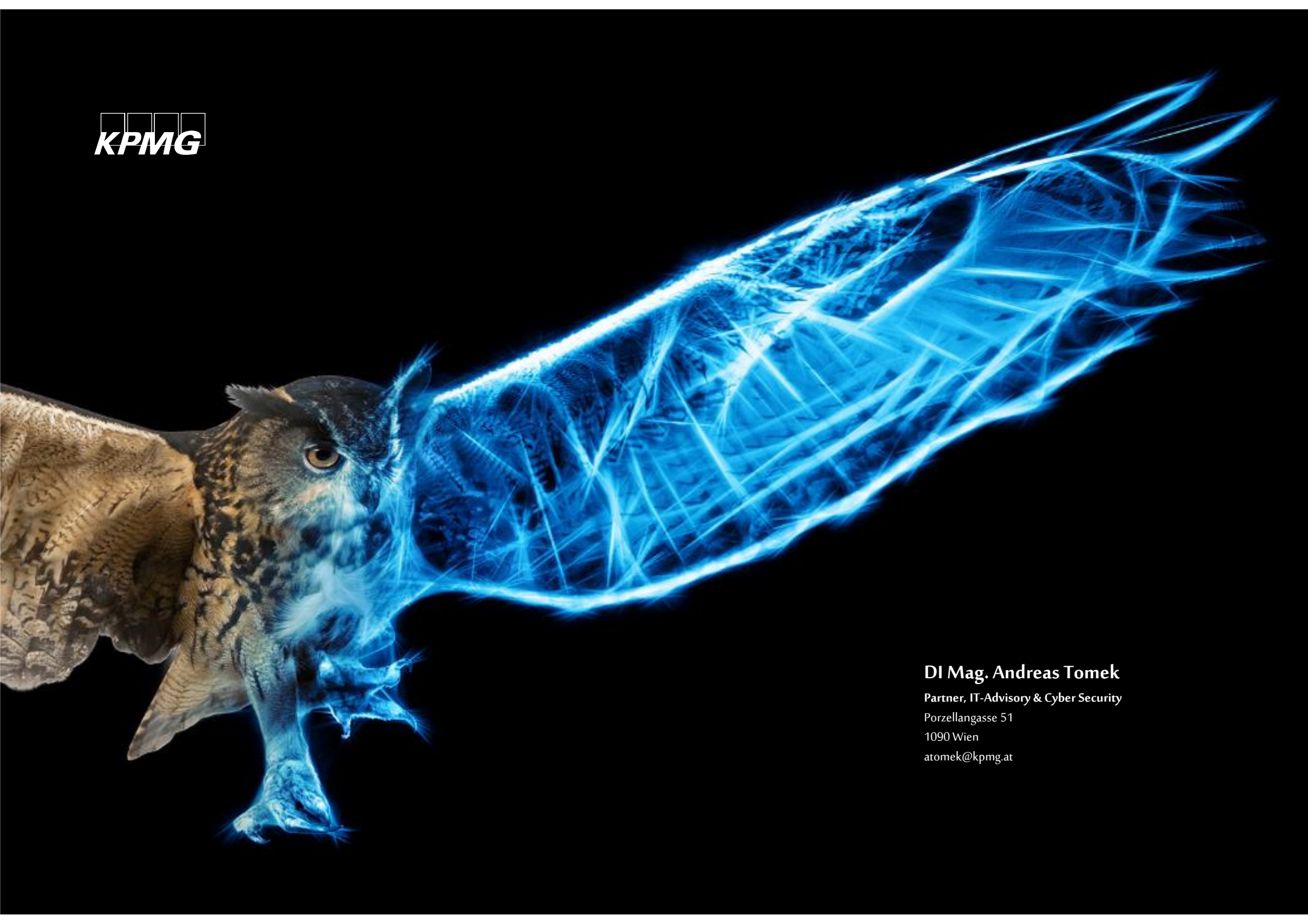


Eine strategische Notwendigkeit

KPMG macht aus Cyber Security eine globale Initiative für strategisches Wachstum. Wir sehen Cyber als einen priorisierten Investitionsbereich und haben uns entschlossen, die weltweit wegwei-senden Standards mit zu gestalten.

KPMG Cyber AT als Teil eines Netzwerkes

Unsere Cyber- Spezialisten in Österreich arbeiten als Team mit hunderten Kollegen weltweit. Darüber hinaus ergänzen wir unsere Teams mit Kollegen aus den Bereichen der IT-Compliance-, CIO- und ERP-Beratung.



DI Mag. Andreas Tomek

Partner, IT-Advisory & Cyber Security

Porzellangasse 51

1090 Wien

atomek@kpmg.at