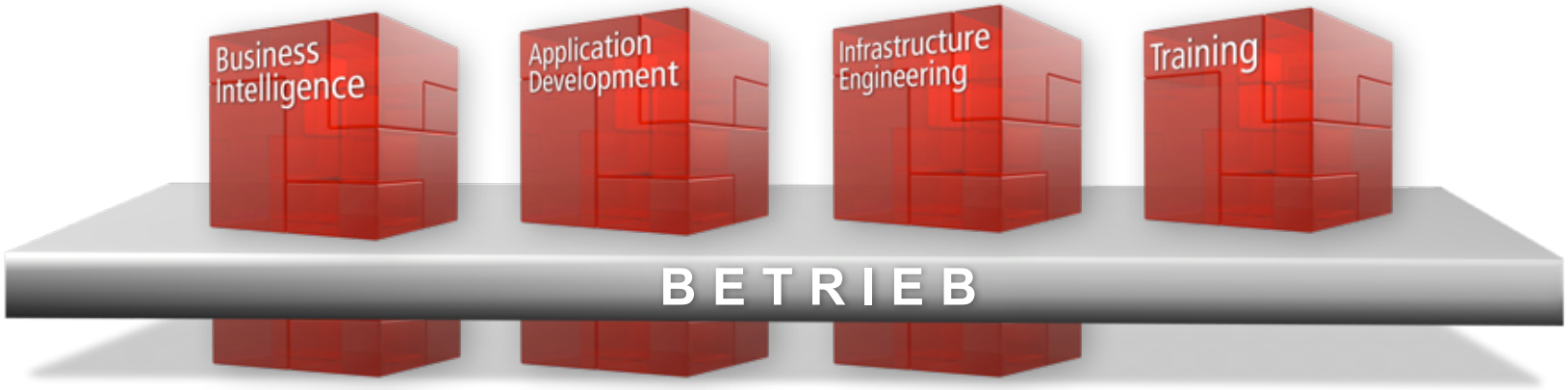
# Die neue EU Datenschutzverordnung

## Konsequenzen für die IT der Unternehmen

**Aleksander Widera**
**Stefan Oehrli**

# Unser Unternehmen.

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE - und Microsoft -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:




Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

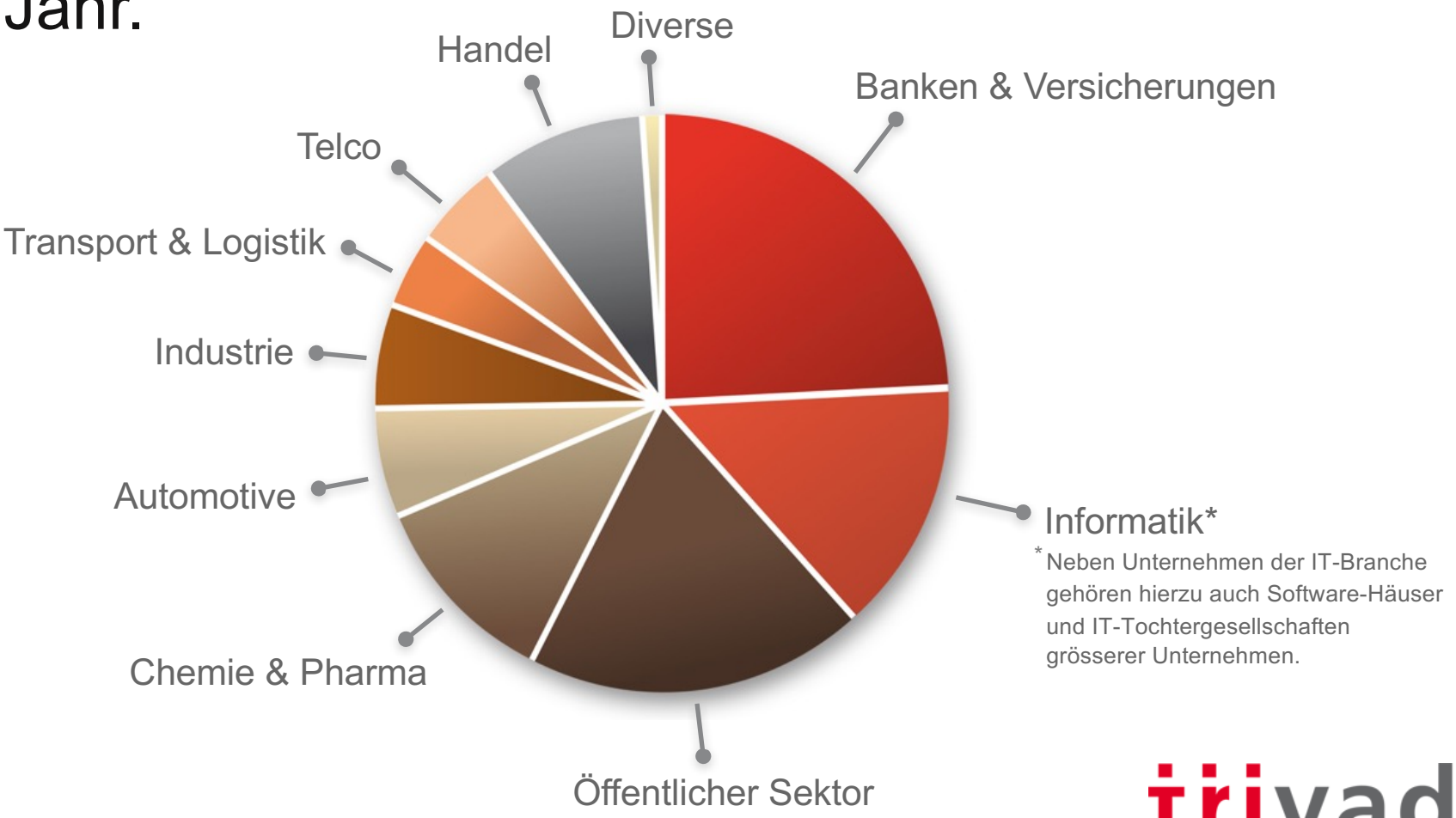
trivadis
makes IT easier.

# Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.

- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis
makes IT easier.

# Unsere Fachkompetenz aus über 1'900 Projekten pro Jahr.




*Neben Unternehmen der IT-Branche gehören hierzu auch Software-Häuser und IT-Tochtergesellschaften grösserer Unternehmen.

trivadis
makes IT easier.

# Stefan Oehrli

**Solution Manager BDS SEC**

- Seit 1997 im IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

**IT Erfahrung**

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogener Umgebungen
- Datenbank Teamleiter

**Spezialgebiet**

- Datenbank Sicherheit Security und Betrieb
- Security Konzepte
- Security Reviews
- Oracle Backup & Recovery

**Skills**

- Backup & Recovery
- Oracle Advanced Security
- Audit Vault und Database Firewall, Database Vault
- Team / Projekt Management

trivadis makes IT easier.

# Aleksander Widera

**IT-Security Consultant & Datenschutzbeauftragter**

- Seit 2004 im IT-Bereich tätig
- Seit 2011 spezialisiert auf IT-Security
- Seit 2014 Datenschutzbeauftragter der Trivadis

**IT Erfahrung**

- Consultant für Security Lösungen
- Technische Unterstützung von Security-Projekten

**Spezialgebiet**

- Cyber Security Solutions - Data Leakage Prevention
- Informationssicherheit
- Secure Programming

**Skills**

- Datenschutz
- Ethical Hacking
- Pentesting

trivadis makes IT easier.

# Technik allein bringt Sie nicht weiter.

## Man muss wissen, wie man sie richtig nutzt.

trivadis
makes IT easier.

# Agenda

1. **Die neue Datenschutz-Grundverordnung**
   - Grundinformationen und Motivation
   - Was ist neu für IT Unternehmen?

2. **Auswirkung auf die Datenbanken**
   - Sicherheit und Compliance der Datenbanken

3. **Konsequenzen der neuen Datenschutz-Grundverordnung**
   - Was müssen IT Unternehmen jetzt tun?



trivadis
makes IT easier.

# Die neue Datenschutz-Grundverordnung



trivadis makes IT easier.

# Datenschutz-Grundverordnung EU 2016/679 (DSGVO)

- Trat am 24. Mai 2016 in Kraft (Art. 99 Satz 1)
  - Geltung unmittelbar in allen EU-Mitgliedsstaaten
  - Bisher Datenschutzrichtlinie 95/46 EG
  - Umgesetzt im Bundesdatenschutzgesetz (BDSG)

- Wirksam erst ab dem 25. Mai 2018 (Art. 99 Satz 2 DSGVO)
  - Bis dahin muss die Verarbeitung personenbezogener Daten und die Datenschutzprozesse umgestellt sein (Schutzzeitraum von 2 Jahren)
  - Öffnungsklauseln ermöglichen, bestimmte Aspekte im nationalem Recht zu regeln



trivadis makes IT easier.

# Datenschutz-Grundverordnung (DSGVO) EU 2016/679

Zielsetzung (Erwägungsgrund 11):

- Vereinheitlichung der Datenschutzgesätze für alle Länder der Europäischen Union
- Stärkung der Rechte der Betroffenen sowie Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten
  - Im Falle eines Verstosses einheitliche Sanktionen auf europäischer Ebene



trivadis
makes IT easier.

# Motivation



trivadis
makes IT easier.

# Sanktionsrahmen

Massive Verschärfung des Sanktionsrahmens

Deutlich erhöhte Bußgelder für Unternehmen von bis zu 4 % des weltweiten Jahres-Umsatzes bei erheblichen Verstößen

- Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen in jedem Einzelfall **wirksam**, verhältnismäßig und **abschreckend** ist (Art 83. Abs. 1)

- Bisher
  - bei schwerwiegenden Verletzungen von Datenschutzvorschriften maximal Bußgeld von bis zu 300.000 €



trivadis makes IT easier.

# Massive Verschärfung des Sanktionsrahmens

- bis **10 Mio. €** oder bis 2% des weltweiten Vorjahresumsatzes (Art. 83 Abs. 4), je nachdem was höher ist
  - Bei Verstößen gegen Regelungen wie z. B.:
  - Grundsätze (Art. 5, z. B. Zweckbindung, Datenminimierung, Speicherbegrenzung)
  - Einwilligung
  - Rechte Betroffener
  - Drittlands Übermittlung
  - Zusammenarbeit mit der Aufsichtsbehörde



trivadis makes IT easier.

# Massive Verschärfung des Sanktionsrahmens

- bis **20 Mio. €** oder bis 4% des weltweiten Vorjahresumsatzes (Art. 83 Abs. 5 & Abs. 6), je nachdem was höher ist
  - Bei Verstößen gegen Regelungen wie z.B.
    - Schutzmaßnahmen (technisch-organisatorische Maßnahmen)
    - Auftragsdatenverarbeitung (NEU: auch gegen Auftragsdatenverarbeiter)
    - Verzeichnis der Verarbeitungstätigkeiten
    - Datenschutz-Folgenabschätzung
    - Bestellung eines Datenschutzbeauftragten
  - Bei Verstößen gegen Anordnungen der Aufsichtsbehörde



trivadis makes IT easier.

# Was ist neu für IT Unternehmen?



trivadis
makes IT easier.

# Was ist neu für IT Unternehmen?

- Jedes Unternehmen, das personenbezogene Daten von Betroffenen verbreitet, die sich in der Europäischen Union befinden, muss die Bestimmungen der DSGVO einhalten (Art. 3)
  - Auch Unternehmen die **keine** Niederlassung in der EU besitzen
  - In der Praxis macht das die DSGVO zu einem weltweitem Gesetz



trivadis
makes IT easier.

# Was ist neu für IT Unternehmen

- Neue, breitere Definition von **personenbezogenen Daten** (Art. 4 Abs. 1)
  - alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen
  - Insbesondere mittels Zuordnung
    - Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung, zu besonderen Merkmalen
    - „Ausdruck der physischen, physiologischen, **genetischen**, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität“



trivadis makes IT easier.

# Auftragsdatenverarbeitung

- Bisher BDSG
  - Haftung des Auftraggebers gegenüber Betroffenen (§ 11 Abs. 1 BDSG)
  - Bußgeld nur gegen Auftraggeber (§ 43 Abs. 1 Nr. 2b BDSG)
- Auftragsverarbeiter als Verantwortlicher bei Festlegung von Zweck und Mittel durch Auftragsverarbeiter (Art. 28 Abs. 10)
  - Klagemöglichkeit der Betroffenen gegen Auftraggeber (Verantwortliche) und gegen Auftragsverarbeiter (Art. 79 Abs. 2)
  - Schadensersatzanspruch der Betroffenen gegen Auftraggeber (Verantwortliche) und gegen Auftragsverarbeiter (Art. 82)



trivadis makes IT easier.

# Auftragsdatenverarbeitung

- Wahrscheinlich zukünftige Praxis:
  - vertragliche Abgrenzung der Verantwortungen
  - vertragliche Klarstellung bzgl. Bestimmung der Zwecke/Mittel
  - vertragliche Haftungsregelungen
  - höhere Dienstleistungkosten durch höheres Risiko



trivadis makes IT easier.

# Sicherheit der Verarbeitung (Art. 32)

Umsetzung durch geeignete technische und organisatorische Maßnahmen

- «Unter Berücksichtigung des **Stands der Technik»**
- Der Implementierungskosten
- Der Art, des Umfangs, der Umstände und dem Zweck der Verarbeitung
- Unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten der Betroffenen
  - Risikobewertung in Zukunft eine zentrale Rolle beim Datenschutz?
- Explizite Erwähnung der Pseudonymisierung und **Verschlüsselung** personenbezogener Daten



trivadis makes IT easier.

# Auswirkung auf die Datenbanken



trivadis
makes IT easier.

# Data Security

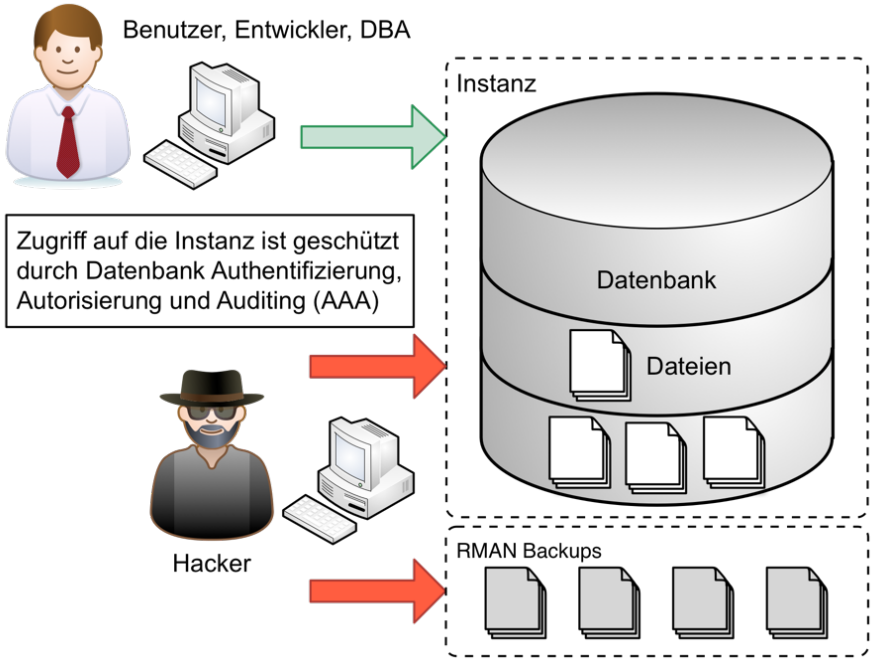
- Artikel 5 beschreibt die Grundsätze für die Verarbeitung der personenbezogenen Daten. Abs. 1 Pkt. f) führt den Grundsatz der „Integrität und Vertraulichkeit“ der personenbezogenen Daten ein
  - Die Verarbeitung personenbezogener Daten muss
  - eine angemessene Sicherheit gewährleisten (Stand der Technik)
  - Schutz vor unbefugter oder unrechtmäßiger Verarbeitung
  - Unbeabsichtigter Verlust, Zerstörung oder Schädigung



trivadis makes IT easier.

# Data Security – Mögliche Massnahmen

- Basis Schutz der Datenbank
  - Authentifizierung, Kerberos, SSL
  - Autorisierung, Rollen Konzepte
  - Auditing, Basis Überwachung
  - Datenbank Härtung
- Identity und Access Management
  - Regelung des Zugriffs und der Rechte
  - Benutzerverwaltung in einem zentrallen Directory






trivadis makes IT easier.

# Data Security – Mögliche Massnahmen

- Trennung der Verantwortlichkeiten
  - Rollentrennung, Benutzer, Operator, Administratoren
  - Database Vault
  - Firewall / Database Activity Monitoring
- Verschlüsselung
  - Netzwerkverschlüsselung (Basis)
  - Verschlüsselung im Speicherort / Ablage (TDE als Option / Feature)
  - Verschlüsselung in der Applikation und somit indirekter Zugriffsschutz



trivadis makes IT easier.

# Data Security – Mögliche Massnahmen

- Sicherer Betrieb der Datenbanken
  - Regelmässiges einspielen der Security Updates
  - Regelmässiger Review der Konfiguration
  - Backup & Recovery Konzept inklusive regelmässigen Tests
  - Angemessene Hochverfügbarkeitslösung



trivadis
makes IT easier.

# Privacy by Design

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25)

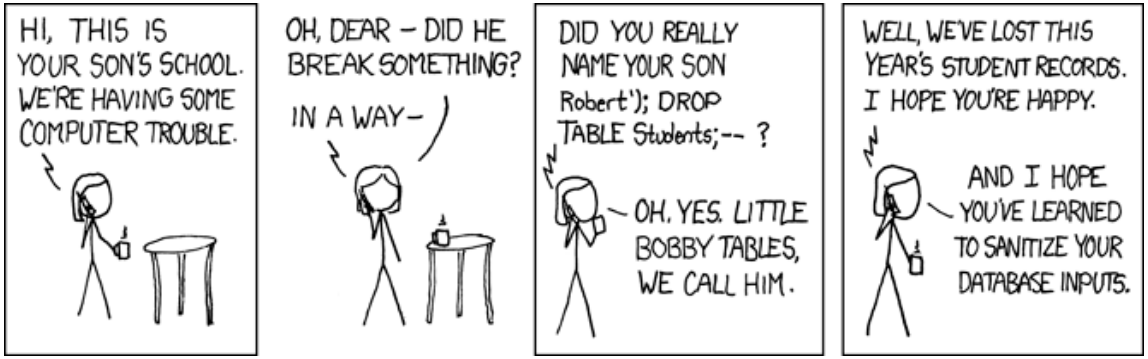
- Datenschutzfördernde Technologien und datenschutzfreundliche Voreinstellungen zur Verarbeitung personenbezogener Daten sollen bereits in der Design-Phase berücksichtigt werden
  - Pseudonymisierung, Datenminimierung, Speicherfrist, Zugänglichkeit
  - Zertifizierung soll erleichtern die PbD Ziele zu erreichen



trivadis makes IT easier.

# Privacy by Design – Mögliche Massnahmen

- Sichere Programmierung
  - Ist die Applikation sicher?
  - Wurden grundlegende Best Practice umgesetzt?
  - Review des Codes / Anwendung
- Ausweisung und Dokumentation der Sensitiven Daten
- Anonymisierung und Maskierung der Sensitiven Daten
  - In der Produktion bei der Ausgabe z.B. Kredit Karten
  - Anonymisierung von Test und Entwicklungsdaten






trivadis makes IT easier.

# Privacy by Design – Mögliche Massnahmen

- Transparent Sensitive Data Protection
  - Oracle Feature
- Authentifizierung und Autorisierung
  - Starke Authentifizierung wie Kerberos, Radius oder mit Zertifikaten
  - Verwendung eines zentralen Directories
- Datenverschlüsselung
  - Im Speicher Ort durch Verschlüsslung der Datafiles und Einsatz von TDE
  - Auf dem Transport Weg durch Netzwerkverschlüsselung



trivadis makes IT easier.

# Privacy Impact Assessment

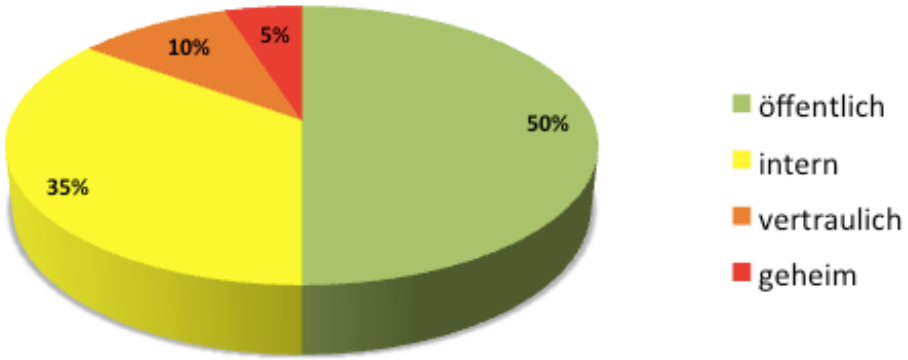
- Könnte die Verarbeitung der personenbezogenen Daten (aufgrund von Art/ Umfang/ Zweck) ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge haben
  - Muss vorab eine Datenschutz-Folgenabschätzung durchgeführt werden
- Dokumentation der eingesetzten Abhilfemaßnahmen zur Eindämmung des Risikos, einschließlich Nachweisanforderungen
- bei Verstoß: Sanktionsrahmen bis 10 Mio. €/ 2 % des Vorjahresumsatzes



trivadis makes IT easier.

# Privacy Impact Assessment – Mögliche Massnahmen

- Wo oder was sind die sensitiven personenbezogenen Daten?
  - Security Assessment und Review der Datenbanken
  - Klassifizierung der Daten respektive Datenbanken
- Datenschutz-Folgenabschätzung
  - Risk Assessments, First Cut Analyse, ...
- Sicherheitskonzept
  - Dokumentation der Massnahmen
  - Umsetzung Datenbank Sicherheit
  - Betrieb sicherer Datenbanken




trivadis
makes IT easier.

# Privacy Impact Assessment – Mögliche Massnahmen

- Trennung der Verantwortlichkeiten
  - Rollentrennung / Segregation of Duties
  - Database Vault
  - Aktive Überwachung mit Database Activity Monitoring
- Sicherstellung der Nachweisanforderungen durch Auditing
  - Datenbank Audit
  - Audit in den Anwendungen. Protokollierung wer was geändert hat.
  - Database- und Applikationsfirewalls, Database Activitiy Monitoring



trivadis makes IT easier.

# Konsequenzen der neuen Datenschutz-Grundverordnung



trivadis
makes IT easier.

# Big Data

Erweiterter Anwendungsbereich für Big Data Auswertungen unter Verwendung pseudonymer Daten (z.B. Internet of Things, Benutzerprofile bei Connected Car). Bislang nur in Ausnahmefällen möglich

- Pseudonymisierung ermöglicht erweiterte Datenverarbeitung
- Beispiel: Nutzungsstatistiken

- Für weitere Informationen laden wir zum nachfolgenden Vortrag von Florian van Keulen «Privacy & Security im Big Data Umfeld» ein



trivadis makes IT easier.

# Cloud Business

Zertifizierung erleichtert den Nachweis der Compliance z.B. für Cloud-Anbieter und kann damit administrative Aufwände erheblich reduzieren.

- Compliance von Cloud-Lösungen nach DSGVO kann durch Zertifizierung nachgewiesen werden
  - Erleichtert Zusammenarbeit mit Partnern
  - Beispiel: Aufwände der Überprüfung der Datenschutz Compliance in z. B. App Store Märkten können durch Zertifizierungen reduziert werden



trivadis makes IT easier.

# Was müssen Unternehmen jetzt tun?

- Analyse
  - Umsetzungszeitraum für DSGVO beträgt zwei Jahre
  - Prüfung aller relevanten Unternehmensprozesse auf Einhaltung der Regelungen
- Implementierung
  - Aufsetzen eines Umsetzungsprojekts
  - Einbeziehung aller betroffenen Unternehmen einer Unternehmensgruppe
- Check
  - Compliance-Prüfung vor Ablauf der Implementierungsfrist



trivadis makes IT easier.

# Zertifizierung

Art. 42 – Zertifizierungen zum Nachweis der Compliance mit den Anforderungen aus der DSGVO

- Die Klassifizierung als Europäisches Datenschutzsiegel ist nach Abs. 5 möglich.

- Dadurch höchste Rechtssicherheit und Verlässlichkeit
  - Geeignet auch zum Nachweis eines angemessenen Datenschutzniveaus bei Übermittlungen in Drittländer



trivadis makes IT easier.

# Fazit

- Die neue EU Datenschutz-Grundverordnung bringt einige Herausforderungen
- Die Sicherheitsanforderungen und Auflagen werden verschärft

Wir Unterstützen Sie gerne:

- Bei Security Reviews und Risk Assessments
- Bei der Erstellung von Sicherheitskonzepten und bei deren Umsetzung
- Bei der ganzheitliche Beratung von Datenbank Sicherheit



trivadis makes IT easier.

# Weitere Informationen...

- Gesetzestext auf http://eur-lex.europa.eu
- Datenschutz relevante Themen in Zukunft Verfolgen
  - Auftragsdatenverarbeitung
  - Zertifizierung



trivadis makes IT easier.

# Weitere Informationen...

- ... zu allen Datenbank bzw. Anwendungs-Security Themen
  http://www.trivadis.com/de/security
- ... zu Schulung DB Betrieb und verschiedenen Security Themen
  http://www.trivadis.com/de/training
- Beratung
  http://www.trivadis.com/de/beratung

**Schwabengipfel Fragebogen Schon ausgefüllt ??**

trivadis
makes IT easier.

# Fragen & Antworten

**Stefan Oehrli**
**Solution Manager / Trivadis Partner**

**Tel. +41 58 459 55 55**
**stefan.oehrli@trivadis.com**

**Aleksander Widera**
**IT Security Consultant**

**Tel. +41 58 459 53 78**
**aleksander.widera@trivadis.com**

Trivadis eXpert Team Security

**http://www.trivadis.com/security**
**http://www.oradba.ch**

Trivadis makes IT easier.



trivadis makes IT easier.