Dateneigentum in Zeiten von GDPR

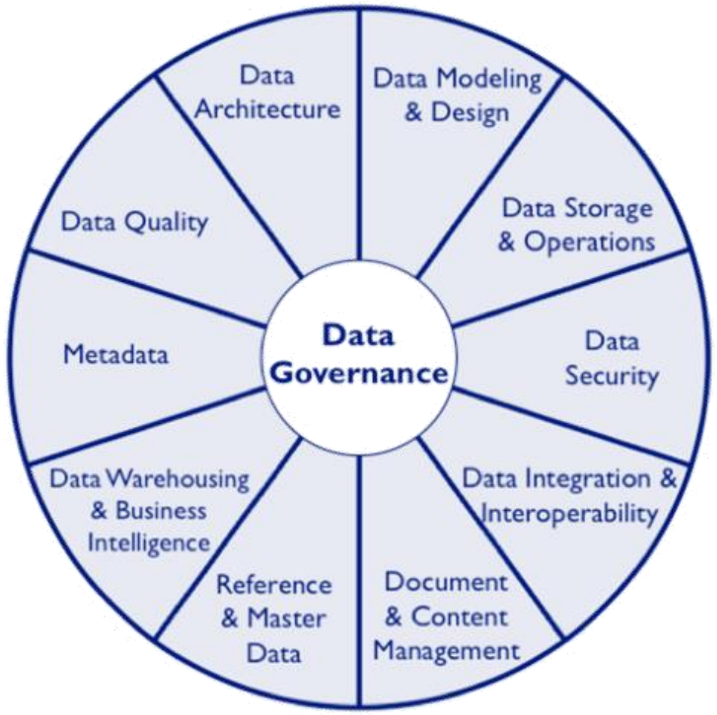
connect Highlightveranstaltung

Dennis Ritter
Baloise Group

26.09.2018

public

Thema



In Zeiten **explodierender Datenmengen** nimmt die Bedeutung einer effektiven Data Governance (u.a. Eigentum) stetig zu. Zu den Treibern gehören neben **datengetriebenen Geschäftsmodellen** und Kosteneffizienz auch der **Datenschutz**. Dieser Kurzvortrag zeigt auf, wie die Baloise Group das Thema **"Datenklassifizierung"** und **"Recht auf Datenlöschung"** als Anforderung aus der neuen EU-Datenschutzgrundverordnung implementiert hat.

Agenda

1. Kurzvorstellung Baloise – Relevanz EU-DSGVO
2. Wesentliche Neuerungen EU-DSGVO
3. Datensicherheitsmassnahmen EU-DSGVO
4. Praxisbeispiel – Datenklassifizierung
5. Praxisbeispiel- Datenlöschung
6. Fragen / Diskussion

Zur Person

- Ausbildung Informatikkaufmann (IHK)
- B.Sc. Wirtschaftsinformatik (DHBW – Villingen Schwenningen)
- Consultant IT-Audit bei PwC Frankfurt und Stuttgart
- Information Security Officer Porsche Financial Services
- Senior Consultant Ernst & Young - Information Security Advisory
- Seit 2015 Senior Information Security & IT-Compliance Officer bei der Baloise Group
- CISA, CISM, CRISC, CISSP, ISO 27001 Lead Implementer

Baloise Group

BELGIUM

Baloise Insurance

Business volume (CHF million)

Life: 143.5 Non-life: 947.1

Investment-type premiums: 470.8

Employees: 1,274

Net combined ratio: 93.4 %

GERMANY

Basler Versicherungen

Business volume (CHF million)

Life: 466.2 Non-life: 755.9

Investment-type premiums: 209.0

Employees: 1,986

Net combined ratio: 109.7

LUXEMBOURG

Baloise Insurance

Business volume (CHF million)

Life: 81.9 Non-life: 116.4

Investment-type premiums: 1,407.3

Employees: 389

Net combined ratio: 93.9 %

SWITZERLAND

Basler Versicherungen Baloise Bank SoBa

Business volume (CHF million)

Life: 2,879.3 Non-life: 1,315.8

Investment-type premiums: 112.1

Employees: 3,621

Net combined ratio: 81.2 %

Wesentliche Neuerungen

EU Datenschutz-Grundverordnung

Rechtmässigkeit der Datenbearbeitung	• Jede Datenbearbeitung erfordert die Einwilligung der Betroffenen oder einen anderen Rechtfertigungsgrund (z. Bsp. Vertragserfüllung, EU-Rechtspflicht, berechtigte Interessen) • Es gelten hohe Anforderungen an die Gültigkeit der Einwilligung • Betroffene müssen umfassend informiert werden (klare, verständliche AGBs)
Rechte der Betroffenen	• Auskunft (auch über automatisierte Entscheidungen und Profiling) • Rückgabe übergebener Daten in elektronischer Form (zwecks Portierung zu einem anderen Anbieter) • Korrektur, Vervollständigung und Löschung (und Weitermeldung des Löschbegehrens bei veröffentlichen Daten) • Aussetzung der Datenbearbeitung • Widerspruch gegen bestimmte Bearbeitungen (z. Bsp. Direktmarketing)
Verantwortlichkeit	• Schaffung einer für die Datenschutz-Governance verantwortliche Stelle (Datenschutzbeauftragter) • Schaffung eines Vertreters in der EU für ausländische Unternehmen • Der für eine Datenbearbeitung Verantwortliche muss belegen können, dass er den Datenschutz einhält • Verzeichnis der Datenbearbeitungen • Datenschutzfolgeabschätzung (und Vorabkonsultation der Aufsichtsbehörde bei hohen Risiken)
Datensicherheit	• Gewährleistung der Datensicherheit durch angemessen technische und organisatorische Massnahmen • Die Datenbearbeitung muss die Einhaltung des Datenschutzes sicherstellen (Privacy by Design) • Standardeinstellungen müssen datenschutzfreundlich sein (Privacy by Default) • Datenschutzverstösse müssen der Behörde (72h) und (bei hohen Risiken) den Betroffenen gemeldet werden
Sanktionen	• Bei Nichtbefolgung können Aufsichtsbehörden Massnahmen oder Sanktionen ergreifen (2-4% des weltweiten Jahresumsatzes oder 10-20 Millionen EUR; es zählt der höhere Betrag) • Betroffene können klagen auf Schadensersatz klagen

Datensicherheitsmassnahmen

EU Datenschutz-Grundverordnung

Governance

- Verantwortlichkeit für Datenschutz und Informationssicherheit
- Gewährleistung der Funktionstrennung
- Sensibilisierung der Mitarbeiter für Datenschutz und Informationssicherheit

Zugang zu den Daten

- Definition und Umsetzung der Zugangsberechtigungen zu Räumlichkeiten (Sicherheit der Arbeitsplätze und Serverräume)
- Zugriffskontrolle auf IT-Systeme und Datenbestände
- Sicherer Zugang von ausserhalb der Organisation (Remote Access)

Lebenszyklus der Daten

- Schutzbedarfsstellung und Klassifizierung von Daten
- Angemessene Sicherheitsmassnahmen zum Schutz der Informationen (Datenerfassung, Protokollierung, Pseudo- oder Anonymisierung, Verschlüsselung)
- Gewährleistung der sicheren Ablage, Sicherung, Archivierung und Vernichtung der Daten
- Sicherheit der Datenträger
- Sicherheit bei der Auslagerung (Bearbeitung durch Dritte)

Datenaustausch

- Netzwerk- und Kommunikationssicherheit
- Signatur und Verschlüsselung von Mitteilungen
- Übergabe von Datenträgern
- Protokollierung des Datenaustausches

Rechte der Betroffenen

- Recht der betroffenen Personen auf Auskunft über und/oder Berichtigung, Sperrung oder Vernichtung ihrer Daten
- Reproduzierbarkeit der Verfahren zur Ausübung des Auskunftsrechts

Datenklassifizierung

Praxisbeispiel

Klassifikationsstufen

Klassifizierung	Beispiele
Öffentlich	• Medienmitteilungen • Allgemeine Geschäftsbedingungen • Geschäftsbericht (einschliesslich Finanzbericht) nach Veröffentlichung • Öffentlich verfügbares Marketing-Material • Veröffentlichte Stellenausschreibungen • Produktbroschüren ……
Intern	• W…ungen • R…emente • Stan…rdarbeitsanweisungen • Al…meine Personendaten: ……
Vertraulich	• Regulato…c… D…en (Daten, die seitens der Aufsichtsbehörden oder des Gese…e…s als …traulich gelten) • IT-Netzwerkdiagra…e und IP-Adressen • Produktspezifikat…en • Besondere Kategorien…ers…bezogener Daten …….
Geheim	• Unterlagen zur Vorstellung d… …lans, der Hochrechnungen und des Abschlusses des Baloise-Konzerns in den Gremien Verwaltungsrat, Konzernleitung sowie für die Bilanzpressekonferenz, die Analystentagung sowie die Generalversammlung • Informationen über sensitive Projekte (insb. M&A) • Geschäftsbericht (einschliesslich Finanzbericht) vor der Veröffentlichung …….

Steigende Anforderungen je nach Klassifikationsstufe

Sicherheitsanforderung

	Öffentlich	Intern	Vertraulich	Geheim
Allgemein				
Identifikation				
Zugriff				
Authentisierung				
Nutzung				
Drucken				
Kopieren / Scannen				
Fotografieren				
Notizen (z.B. Whiteboards)				
Mobiles Arbeiten				
Elektronische Übertragung				
Email				
Datenübermittlung				
Physische Übertragung				
Post, Kurierdienst				
Speicherort				
Elektronisch				
Physisch				
Löschung				
Elektronisch				
Physisch				
Entsorgung				
Speichermedien (z.B. USB-Sticks)				

Art.17 EU-DSGVO – Recht auf Löschung

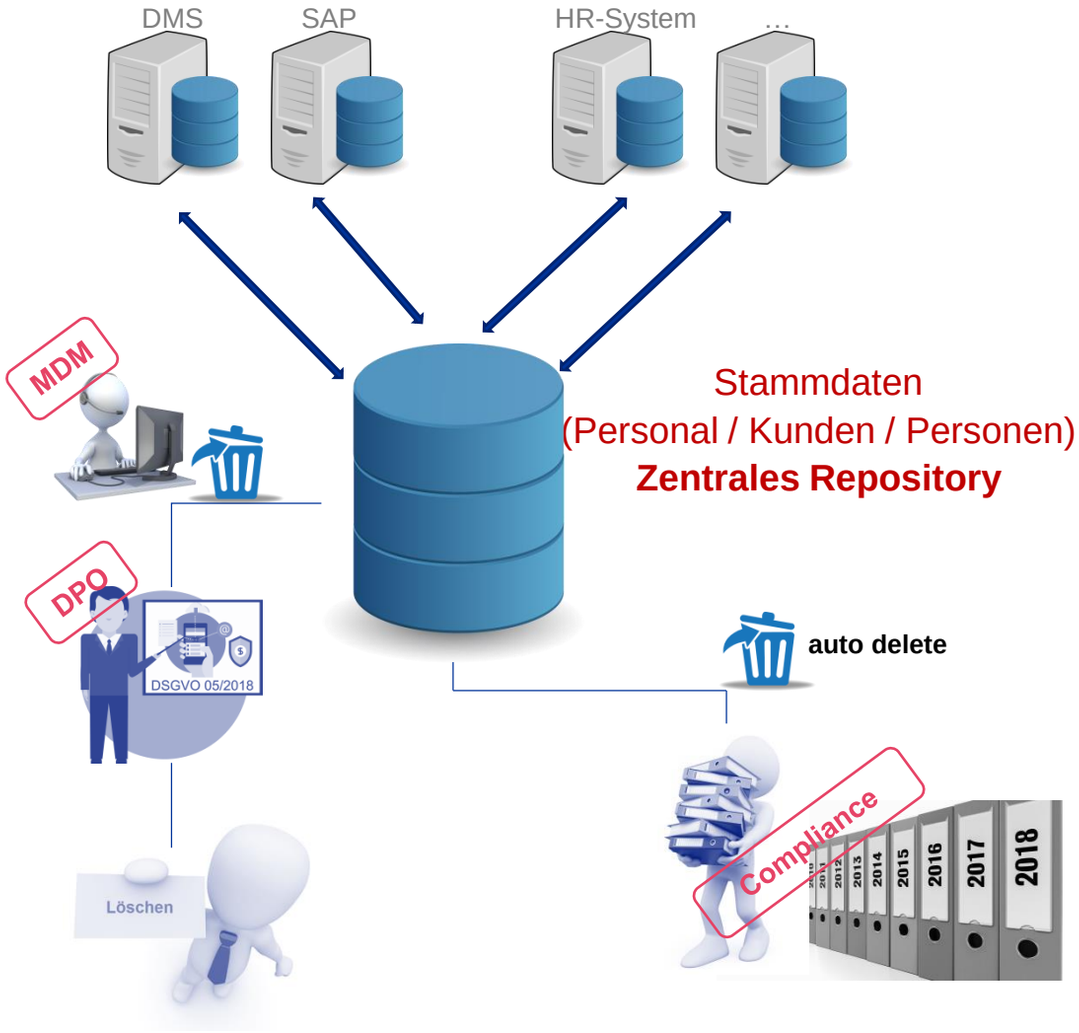
Art.17 – EU-DSGVO – Recht auf Löschung (Recht auf Vergessenwerden)

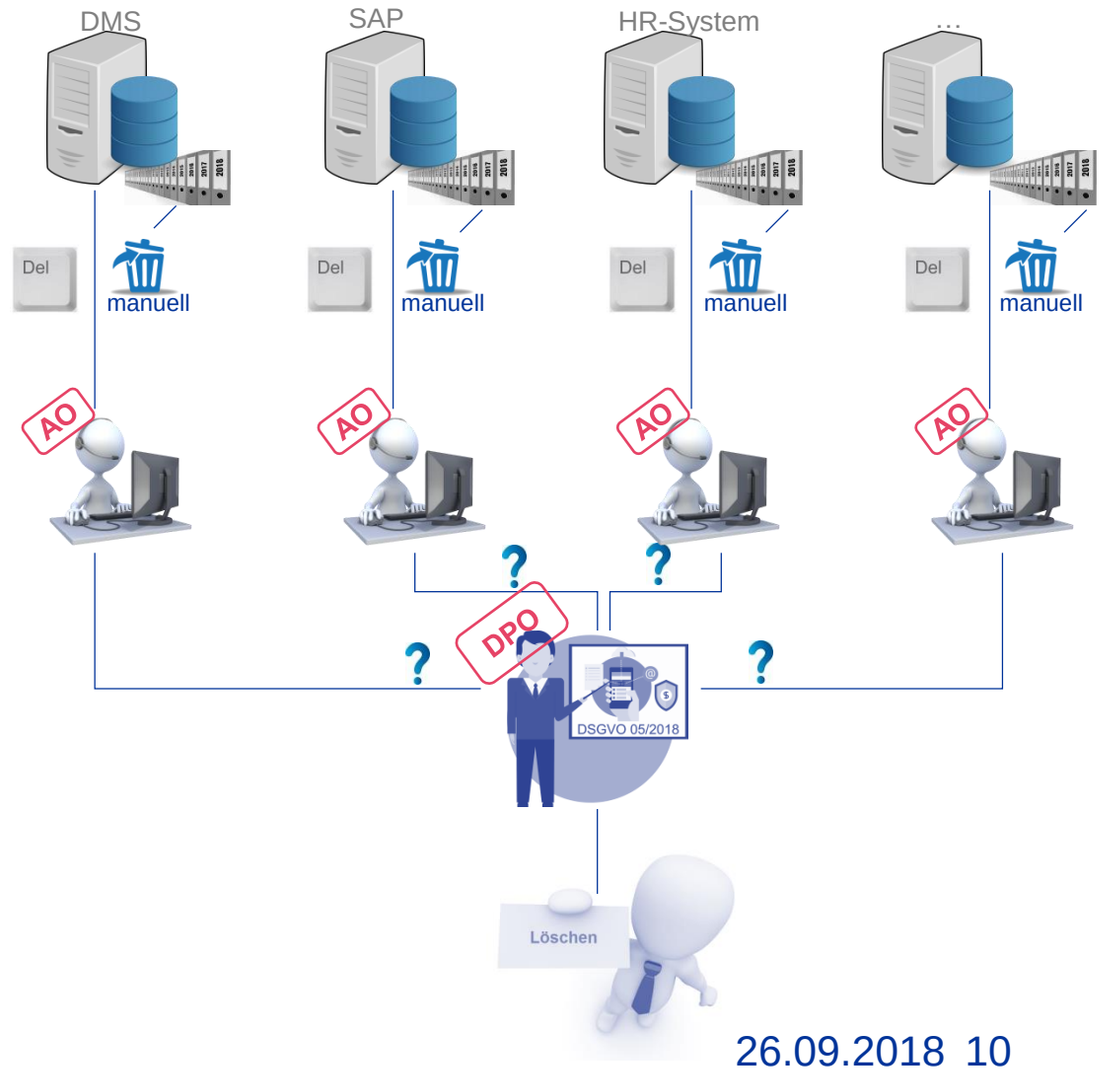
1. Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

Recht auf Löschung - Lösungsansätze





Questions / Remarks

Vielen Dank für Ihre Aufmerksamkeit

Dennis Ritter
Senior Information Security & IT-Compliance Officer
CISA I CISM I CRIC I CISSP
Phone +41 58 285 8446
dennis.ritter@baloise.com