



HERZLICH WILLKOMMEN

DATENSCHUTZ FÜR MICROSOFT 365



ERLEBEN, WAS VERBINDET.

#CLOUD

#AI

#AUTOMATION

DIGITAL TRUST

#IOT

#ETHICS

#14.0

Privacy

Security

Blockchain

Datenschutz

- Datenschutzmanagement-systeme
- Externer Datenschutzbeauftragter
- Datenschutz-auditor
- Datenschutz-beratung
- Technischer Datenschutz (TOM)

Governance, Risk & Compliance

- GRC Consulting (KRITIS, TISAX)
- Risiko-management
- ISMS (ISO27*, BSI)
- Audits & Assessments

Security Consulting & Architecture

- Security Consulting
- CISO / ISB / Security Officer
- Cloud Security
- Privacy Security Services (PSS)
- IAM / CIAM Consulting
- ICSS (Industrie 4.0)
- Container und DevOps Security
- Infrastructure Security

Security Services

- Infrastructure Security Service (WAF / PAM)
- Cloud Data Protection Service
- IAM / CIAM Service
- SOAR Service (SIEM/SOC)
- HoneySens Service

Training & Awareness

- Schulungen / Live-Workshops
- Konzepte / Consulting
- eLearning / WBTs
- Awareness Kampagnen
- Social Engineering
- Micro-Learnings (Mobile App)

Blockchain Solutions Center

- Strategy & Business Model Consulting
- Consortium Build Up
- Co-Creation
- Use Case Consulting & Implementation
- Blockchain Security Assessment
- Blockchain Infrastructure "Made in Germany"

Analyse

Entwerfen

Automatisieren

Messen

Überwachen

Neubeurteilen

Hyperautomatisierung

DS Herausforderungen beim Einsatz M 365

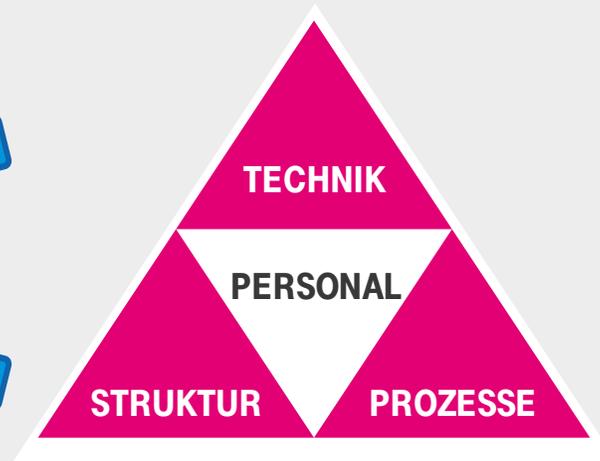
Cloud Compliance

Anforderungen an den Cloud-Einsatz

Datenschutz

- DSGVO / BDSG
 - Datenschutzfolgenabschätzung
 - Auftragsverarbeitung (EU-Standard-Vertragsklauseln)
- SGB Datenschutzanforderungen Sozialdatenverarbeitung

Compliance Anforderungen



Regulatorische Anforderungen

- § 32 Versicherungsaufsichtsgesetz
- VAIT / BAIT
- MaRisk
- Orientierungshilfe der BaFin zu Auslagerungen an Cloud-Anbieter

Security

- Data Governance
- Business Continuity
- Identity & Access Management
- Hardening
- Encryption & Key Management
- Logging & Monitoring

Normen / Standards

- BSI IT-Grundschutz
 - C5 Anforderungskatalog Cloud Dienstleister
- ISO 27001 / ISO 27701
- BSI KRITIS-Verordnung

M365 datenschutzkonform nutzen – aber wie?

Beachtung Artikel 32: Risikobasierter Datenschutz (DSFA!)

Deaktivierung nicht benötigter Dienste

Deaktivierung problematischer Services wie Sway oder Workplace Analytics

Einschränkung von Third Party Apps (In Teams)

Verschlüsselung der Daten in der Cloud / E-Mails

Klassifizierung und Schutzbedarfsfeststellung für die Ablage der Daten in der Cloud

Erstellung erforderlicher Konzepte (z. B. Lösch- sowie Berechtigungskonzept)

Schulung der Mitarbeiter hinsichtlich Umgang mit O365 und welche Informationen abgelegt werden dürfen



Empfehlung: Datenschutz- folgenabschätzung

Datenschutzfolgenabschätzung

Kriterien für Notwendigkeit



GRUNDLAGEN UND ZIELE

Werkzeug für Beschreibung, Bewertung und Begrenzung von Risiken, welche bei der Verarbeitung von pDaten für die Betroffenen bestehen.

Zuständigkeit:
Verantwortliche Stelle
(Art. 35 Abs. 1 S. 1 DSGVO)

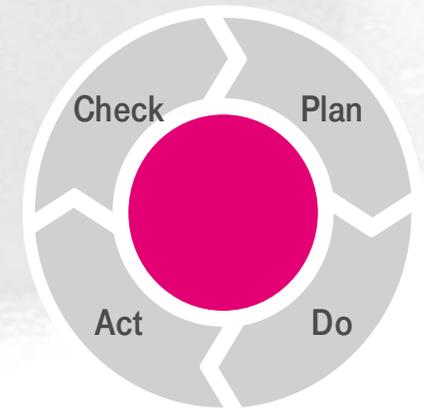
Bei Auftragsverarbeitung:
Unterstützung durch
Auftragsverarbeiter
(Art. 28 Abs. 3 Buchst. f
DSGVO)

Notwendige Betroffenen­sicht:
Ggf. Einbeziehung Betriebsrat
(Art. 35 Abs. 9 DSGVO) ?!

Notwendige Prozesssicht:
Risikobewertung

Nachweispflicht:
DSFA-Bericht

Regelmäßige Prüfung und
Aktualisierung



Datenschutzfolgenabschätzung

Prozessdarstellung



Umsetzung der technisch-organisatorischen Maßnahmen nach DSFA:

- Ggf. Betriebsvereinbarung
- Ergänzung Verarbeitungsverzeichnis
- Dokumentation der vorgenommenen datenschutzfreundlichen Einstellungen bei Microsoft-Produkten
- Lösch- und Protokollierungskonzept
- Rollen- und Berechtigungskonzept
- Nutzungsrichtlinie der Microsoft-Produkte für Mitarbeiter
- Ggf. Schulungskonzept und Schulungsunterlagen für Mitarbeiter des Kunden
- Datenschutzinformationen für Mitarbeiter des Kunden für tägliche Anwendung

Projektvorgehen Datenschutzberatung M365

Wir unterstützen Sie ganzheitlich



Erstanalyse

- Workshop vor Ort oder remote
- Analyse der Anwendungsbereiche, Datenkategorien und Verarbeitungstätigkeiten des geplanten Nutzungsumfanges von M365
- Identifikation der bestehenden und zukünftigen Datenschutzanforderungen

Ergebnis: Erste Risikoindikation und Handlungsempfehlungen



Detaillierte Risikoanalyse

- Durchführung einer umfassenden Datenschutzfolgenabschätzung (DSFA)
- Umfassende Bewertung der Datenschutzrisiken

Ergebnis: DSFA-Bericht inkl. Maßnahmenplanung



Maßnahmenumsetzung

Unterstützung bei der Umsetzung konkreter technischer & organisatorischer Maßnahmen, z. B.:

- Betriebsvereinbarung
- Nutzungsrichtlinie
- Datenschutzaudit
- Security Beratung
- Cloud-Verschlüsselung

Ihre Ansprechpartner



Monika Meinhardt LL.M.
Consultant Data Privacy

Datenschutzbeauftragte (TÜV)
Datenschutzauditorin (TÜV)

T-Systems MMS

+49 30 275 833 8441

monika.meinhardt@t-systems.com



Enrico Weide
Consultant Data Privacy

Datenschutzbeauftragter (TÜV)
Datenschutzauditor (TÜV)

T-Systems MMS

+49 171 8103075

enrico.weide@t-systems.com



Attila Misota
Sales Expert

ISO 27001 Foundation
ITIL Foundation

T-Systems MMS

+49 171 3077245

attila.misota@t-systems.com