



# Grenzen erkennen – Möglichkeiten erweitern

Unternehmens- und IT-Organisationsberatung, Coaching, Mediation,  
Projekt-, Change-, Interimsmanagement, Datenschutzberatung/DSGVO, CSR

## Daten sind der Rohstoff der Zukunft

**Durch die Digitalisierungswelle boomen neue Geschäftsmodelle auf Basis persönlicher Daten. Das Ziel der DSGVO: Der EU-Bürger soll wieder Herr seiner Daten sein, nicht die Datenindustrie!**

Die EU und deren Beitragsländer haben sich dieser Dynamik angenommen. Mit 25. Mai 2018 tritt nach einer 2-jährigen Übergangsfrist die erste EU-weite Datenschutzgrundverordnung (DSGVO) in Kraft. Die DSGVO regelt Europaweit den Umgang mit personenbezogenen Daten. Das Strafausmaß (bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes) für eine Verletzung der DSGVO kann sehr schmerzhaft sein und bis zur Stilllegung der Datenverarbeitung führen. Kommt es zu einer Beschwerde eines Betroffenen bei der Datenschutzbehörde, muss die Organisation die Einhaltung der DSGVO nachweisen. Kann sie das nicht, kann bereits EIN Vorfall zur Überlebensfrage werden.

### Die DSGVO betrifft alle Unternehmen, Vereine, NGOs

In welchem Ausmaß ist abhängig von der Unternehmensgröße, der Datenkategorie und den Risiken.

### Daten sind der Rohstoff der Zukunft, der Datenschutz im Mittelpunkt

Anfang März 2018 wurde beim 12. Europäischen Datenschutntag in Wien durch den BM Hr. Dr. Moser hervorgehoben, dass die Befugnisse der zentralen Datenschutzbehörde (DSBh) massiv aufgewertet wurden. Nachdem sich die Datenmenge alle 2 Jahre verdoppelt, ist es besonders wichtig den Datenschutz in der Praxis zu verstehen um Rechtskonform handeln und daraus resultierende Chancen nutzen zu können.

### DSGVO - Rechtskonformität

Die DSGVO bietet einen Rechtsrahmen, der für alle EU-Staaten gleichermaßen gilt. Unternehmen aus Drittstaaten müssen, wenn Sie Dienstleistungen und Produkte in der EU anbieten, dem Datenschutzniveau der DSGVO entsprechen.

### DSGVO als Chance: Wer sorgsam mit Daten umgeht, schafft Vertrauen und Loyalität

Eine qualitätsvolle Handhabung von Daten, mit vorheriger zweckgebundener Einwilligung, schafft Vertrauen bei Kunden, Mitgliedern, Mitarbeitern und Partnern. Ohne Vertrauen aller Mitwirkenden im gesamten Daten-Lebenszyklus wird es in Zukunft kein nachhaltiges Business geben.

Diese Informations- und Transparenzverpflichtungen bilden einen „elektronischen Handschlag“ und erfordern zugleich, dass sich die Organisationen mit Ihren Wertschöpfungsstrukturen auseinandersetzen müssen (z.B. welche Informationen werden in welchen Prozessen wie verarbeitet). Die DSGVO Prinzipien bieten dazu eine Hilfestellung für technische und organisatorische Optimierungs- und Risikomaßnahmen (Business & IT). Die Einführung eines Datenschutzmanagementsystems ermöglicht zudem umfassende Einsparungs- und neue Geschäftspotenziale.



### Die 7 DSGVO Prinzipien

Unabhängig der Verarbeitungsform von persönlichen Daten müssen die Grundsätze der Rechtmäßigkeit, Zweckgebundenheit und Notwendigkeit erfüllt sein.

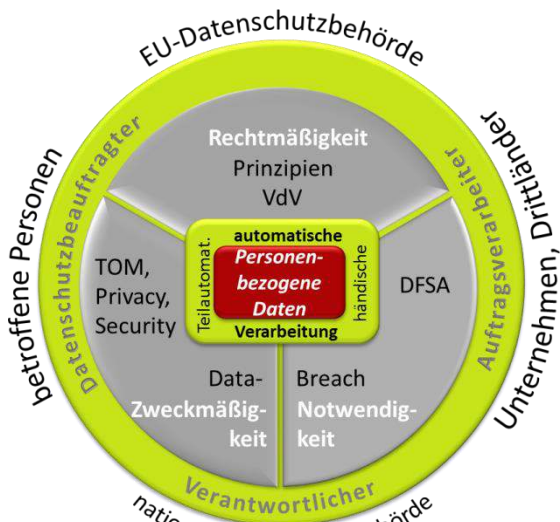


# Grenzen erkennen – Möglichkeiten erweitern

Unternehmens- und IT-Organisationsberatung, Coaching, Mediation,  
Projekt-, Change-, Interimsmanagement, Datenschutzberatung/DSGVO, CSR

## Die DSGVO auf einem Blick

Den Kern der DSGVO bildet die Verarbeitung von personenbezogenen Daten. Der Schutz von betroffenen Personen gilt in allen EU-Staaten gleichermaßen. Nationale Anpassungen sind möglich. Bei Verarbeitungen in Drittländern ist auf ein DSGVO konformes Datenschutzniveau zu achten.



EU-DSGVO, DSG 02/2018, ©Mayr-Consulting.at

Der Verantwortliche im Unternehmen muss für die DSGVO Konformität sorgen, bei entsprechender Verpflichtung einen Datenschutzbeauftragten bestellen (DSB Meldepflicht) und mit allen Auftragsverarbeitern eine verbindliche DSGVO Basis sicherstellen.

Um dieser Verantwortung gerecht zu werden, ist es erforderlich eine Daten- und Anwendungsinventur mit Bedacht auf die DSGVO Prinzipien durchzuführen und ein Verarbeitungsverzeichnis (VdV) zu erstellen.

Besteht ein hohes Risiko für die Rechte und Freiheiten von betroffenen Personen, dann ist eine Datenschutzfolgeabschätzung (DSFA) durchzuführen und risikomildernde technische und organisatorische Maßnahmen (TOM) zu setzen.

Der Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen bei Anwendungen (Privacy by Design, Privacy by Default), Datensicherheit (IT-Security) und durch organisatorische Sicherheitsmaßnahmen muss nachweislich sichergestellt, dokumentiert und überprüft (auditiert) werden. Im Falle einer Datenschutzverletzung – Data Breach (z.B. Verlust des Datenträgers, Hacker, Einbruch) muss der Vorfall der DSBh innerhalb von 72 h gemeldet werden. Ausnahme: Wenn kein Risiko für die Rechte und Freiheiten der Betroffenen besteht.

Darüber hinaus sind Verfahren einzurichten, welche die Bearbeitung der Betroffenenrechte (z.B. Auskunft, Löschung der Daten) unverzüglich bzw. innerhalb eines Monats sicherstellen. Erfolgt dies nicht, kann der Betroffene eine Beschwerde bei der DSBh einreichen. Die DSBh muss jeder Beschwerde nachgehen und innerhalb von drei Monaten dem Beschwerdeführer über den Ermittlungsstatus unterrichten. Dazu fordert die DSBh vom Verantwortlichen den Nachweis zur Einhaltung der DSGVO (z.B. Verarbeitungsverzeichnis, Datenschutzrisikobewertung, Dokumentation, Audits) ein.

**Fazit: Wenn Organisationen nicht über die erforderliche Ressourcen verfügen, dann ist es absolut empfehlenswert einen externen Datenschutzbeauftragten beizuziehen. Nichts tun ist keine Option.**

Die Einführung einer Datenschutzorganisation erfordert neben Recht & IT Wissen, spezielle Kompetenzen in der Organisationsentwicklung und im Umgang mit Veränderungen. Nur mit einer ganzheitlichen Vorgehensweise kann ein nachhaltiger Mehrwert für die Organisation und deren Stakeholder sichergestellt werden.

Ein externer Datenschutzbeauftragter gemäß Art. 39 DSGVO kann Umwege und Kosten sparen.



### Mayr Gerald, MBA, MSc

Unternehmensberater und Segel-Coach ([www.segelerlebnis.at](http://www.segelerlebnis.at))  
Zertifizierter Datenschutzbeauftragter (DSGVO, DSG 2018), TÜV-SÜD  
Zertifizierter, eingetragener Wirtschaftsmediator nach ZivMediatG BGBL. 29/2003  
Akkreditierter CSR-Experte, WKO/Incite