

Richtiger Umgang mit der Datenschutz-Grundverordnung

Toolset DSGVO D_00a Einführungspräsentation

Hinweis: Diese Musterpräsentation dient der allgemeinen Erstinformation zu den Regelungen der DSGVO. Dieses Muster ist an die Bedürfnisse der des jeweiligen Unternehmens individuell anzupassen.

Dieses Muster wurde mit größter Sorgfalt erstellt, für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster erstellt haben, sind daher ausgeschlossen.

Grundlagen des
Datenschutzes

Datenschutz-Grundverordnung (DSGVO)

wesentliche Begriffe iZm
der DSGVO

→ **die DSGVO gilt ab dem 25.05.2018**

Akteure im Datenschutz

- EU-Verordnung und somit in den Mitgliedstaaten **unmittelbar anwendbar**
 - Verordnung gilt, ohne dass es eines nationalen Umsetzungsaktes bedarf
 - steht eine Verordnung im Konflikt mit einem nationalen Gesetz → Verordnung hat Vorrang

Zulässigkeit
Datenverarbeitung

Exkurs: Einwilligung

DSGVO – was haben
Unternehmer zu
beachten?

→ zahlreiche **Öffnungsklauseln** → **nationale Regelung** durch die einzelnen Mitgliedstaaten

Einsatz von
Auftragsverarbeitern

→ Datenschutzrecht wird EU-weit vereinheitlicht

Datenübermittlung an
Drittländer

→ Rechtsgrundlage der **Datenverarbeitung**

Datenübermittlung
zwischen
Konzerngesellschaften

Arbeitnehmerdatenschutz

Checkliste

Grundlagen des
Datenschutzes

Datenschutz-Grundverordnung (DSGVO)

wesentliche Begriffe iZm
der DSGVO

→ **Ausweitung** der **Rechte** der Betroffenen und **Pflichten** der Verantwortlichen

Akteure im Datenschutz

→ Erweiterung der Befugnisse der Behörden

Zulässigkeit
Datenverarbeitung

→ **Verschärfung der Sanktionen**

Exkurs: Einwilligung

→ Geldbußen bis zu **EUR 20 Mio.** bzw. **4 % des weltweiten Vorjahresumsatzes** (je nachdem, welcher Betrag höher ist)

DSGVO – was haben
Unternehmer zu
beachten?

→ **Datenschutz-Anpassungsgesetz („DSG neu“)** tritt mit **25.05.2018** in Kraft

Einsatz von
Auftragsverarbeitern

→ nationales ö Gesetz

Datenübermittlung an
Drittländer

→ Konkretisierung der DSGVO in einzelnen Punkten

→ kein gänzlich neues Gesetz, sondern **Novellierung** des bereits bestehenden **Datenschutzgesetzes 2000**

Datenübermittlung
zwischen
Konzerngesellschaften

→ **Datenschutz-Deregulierungsgesetz 2018**

Arbeitnehmerdatenschutz

→ Ua Verwarnen statt strafen

Checkliste

→ Ua Aufweichung des Auskunftsrechts

Grundlagen des
Datenschutzes

wesentliche Begriffe iZm
der DSGVO

Akteure im Datenschutz

Zulässigkeit
Datenverarbeitung

Exkurs: Einwilligung

DSGVO – was haben
Unternehmer zu
beachten?

Einsatz von
Auftragsverarbeitern

Datenübermittlung an
Drittländer

Datenübermittlung
zwischen
Konzerngesellschaften

Arbeitnehmerdatenschutz

Checkliste

Exkurs: Haftung, Schadenersatz und Geldbußen (Art 82 und 83)

– Strafen

- „Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein“
- Verletzung von Pflichten des Verantwortlichen
 - Bis EUR 10 Mio (bzw 2 % des Konzernumsatzes)
 - Verletzung der TOMs
 - Verletzung der Vorschriften zum Verarbeitungsverzeichnis
 - Verletzung der Vorschriften zur Datenschutzfolgenabschätzung
 - Verletzung von Rechten des Betroffenen
 - Bis EUR 20 Mio (bzw 4 % des Konzernumsatzes)
 - Verletzung von Rechten betroffener Personen
 - Verstoß gegen die rechtmäßige Verarbeitung
 - Verletzung der Bestimmungen betreffend internat. Datenverkehr

– Schadenersatz

- Verantwortlicher haftet
 - Gegenüber jeder Person der ein materieller oder immaterieller Schaden entstanden ist (Kosten, Verdienstentgang, Schmerzensgeld)
 - Bei einem Verstoß gegen die DSGVO
- Auftragsverarbeiter haftet nur für seine speziellen Pflichten
 - Müssen vertraglich geregelt sein

Grundlagen des Datenschutzes

→ § 1 Datenschutzgesetz 2000 (derzeit geltende Fassung)

„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.“

→ im **Verfassungsrang** verankertes **Grundrecht**

→ „DSG neu“ lässt die Anwendbarkeit der Verfassungsbestimmungen des DSG 2000 unberührt

Grundlagen des Datenschutzes

→ **Datenverarbeitung grundsätzlich verboten (Verbotsprinzip)!**

→ **Ausnahmen** von diesem Verbot?:

- ausdrückliche gesetzliche Ermächtigung oder Verpflichtung
- Erfüllung eines Vertrags mit der betroffenen Person
- Zustimmung des Betroffenen
- lebenswichtige Interessen des Betroffenen (zB medizinische Behandlung)
- überwiegend berechtigte Interessen des Verantwortlichen oder eines Dritten
- Daten sind öffentlich oder anonym

wesentliche Begriffe iZm der DSGVO

- Schutzobjekt der DSGVO sind „**personenbezogene Daten**“

*„alle Informationen, die sich auf **eine identifizierte oder identifizierbare natürliche Person („betroffene Person“)** beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“*

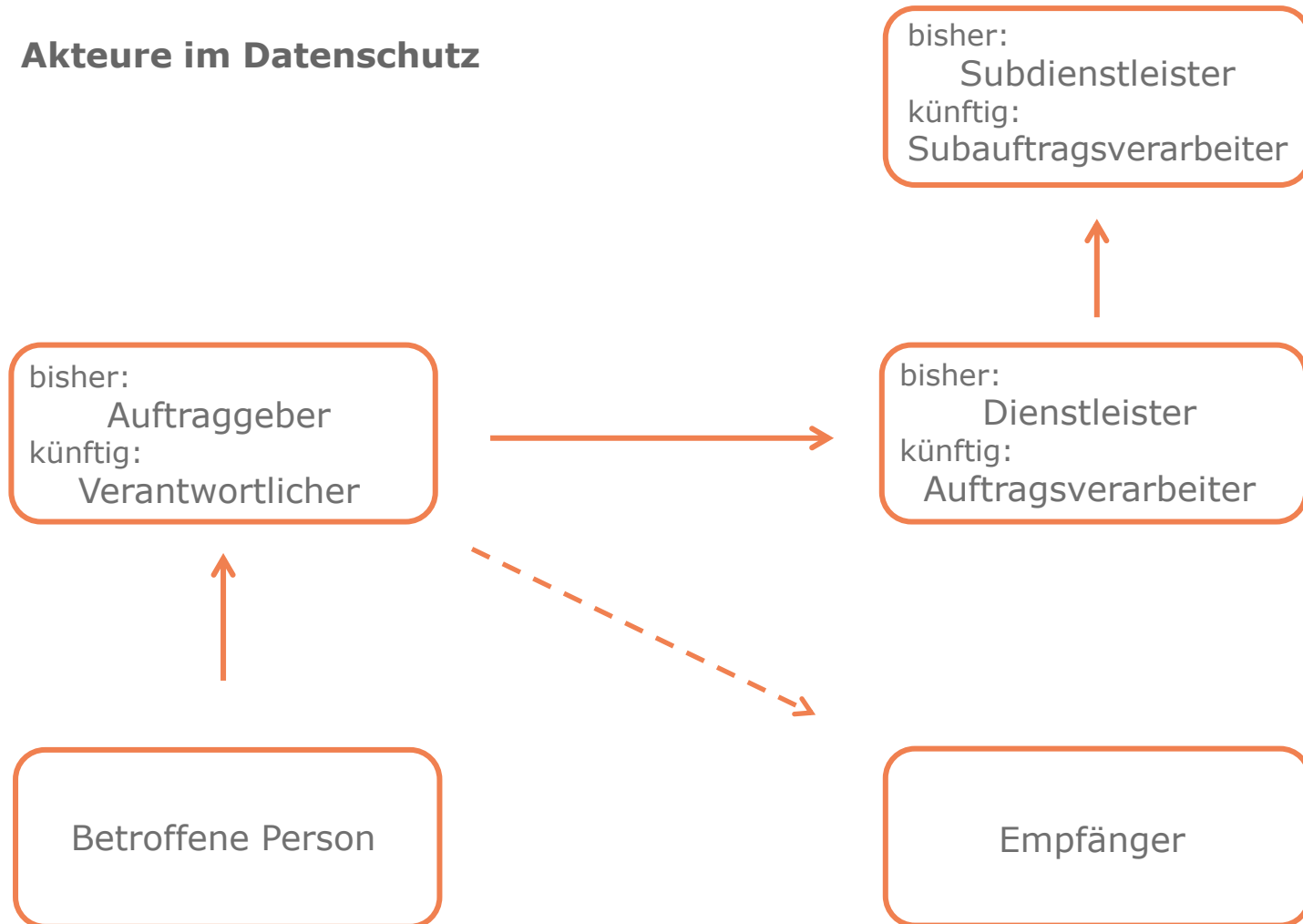
- **pseudonymisierte Daten** fallen in den Anwendungsbereich der DSGVO; **anonyme Daten** hingegen nicht
- besondere Datenkategorien („**sensible Daten**“): Daten natürlicher Personen über deren rassistische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugung, Gesundheit etc.

wesentliche Begriffe iZM der DSGVO

→ Definition „**Datenverarbeitung**“ iSd DSGVO:

*„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie **das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.**“*

Akteure im Datenschutz



Akteure im Datenschutz

- **Verantwortlicher** (bisher Auftraggeber): natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die **Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.**
- **Auftragsverarbeiter** (bisher Dienstleister): natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten **im Auftrag des Verantwortlichen verarbeitet.**
- **Betroffene Person:** jene natürliche Person, auf die sich die personenbezogenen Daten beziehen.

Zulässigkeitsvoraussetzungen für die Datenverarbeitung

- 1. Einhaltung von allgemeinen Datenverarbeitungsgrundsätzen
 - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit

- 2. Rechtmäßigkeit der Datenverarbeitung
 - **Einwilligung, Vertragsanbahnung / Vertragserfüllung**, Erfüllung rechtlicher Verpflichtungen, Schutz lebenswichtiger Interessen, Öffentliche Interessen, Berechtigte Interessen (Interessensabwägung)

Exkurs: Einwilligung

- **Einwilligung** nach der DSGVO ist eine
 - freiwillig,
 - für den bestimmten Fall (keine Pauschaleinwilligungen),
 - in informierter Weise und
 - unmissverständlich abgegebene Willensbekundung (schriftlich!).
- bei **Ungleichgewicht** (Arbeitgeber, Arbeitnehmer) oder bei **Koppelung** einer datenschutzrechtlichen Zustimmung an einen Vertragsabschluss kann es an der **Freiwilligkeit fehlen**
- **Widerrufsmöglichkeit**
- **Beweislast** liegt beim Verantwortlichen

In Anbetracht der jederzeitigen Möglichkeit des Widerrufs sollte eine Verarbeitung personenbezogener Daten im unternehmerischen Bereich nur im Ausnahmefall (nur) auf eine Einwilligung gestützt werden.

DSGVO – was haben Unternehmer zu beachten?

- Verzeichnis von Verarbeitungstätigkeiten
 - die generelle DVR-Meldepflicht entfällt mit der DSGVO
 - stattdessen ist ein Verzeichnis zu führen, welches auf Anfrage der **Aufsichtsbehörde vorzulegen** ist
 - bei weniger als 250 Mitarbeitern, nur wenn die Verarbeitung ein **Risiko** für Rechte der Betroffenen birgt oder **nicht nur gelegentlich** erfolgt oder **sensible** Daten betrifft

DSGVO – was haben Unternehmen zu beachten?

– Datenschutz-Folgenabschätzung

- Auswirkungen und Risiken der Datenverarbeitungen sollen für die Rechte der Betroffenen analysiert und die Folgen der vorgesehenen Datenverarbeitungen für den Datenschutz abgeschätzt werden
- wenn etwa neue Technologien verwendet werden oder aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** besteht
- ergibt die Folgenabschätzung ein hohes Risiko → Vorab-Konsultation der Aufsichtsbehörde
- Entwurf der „White List“ (= keine Folgenabschätzung) wurde Anfang April publiziert

DSGVO – was haben Unternehmen zu beachten?

- Bestellung eines Datenschutzbeauftragten
 - interne Beratungs- und Kontrollfunktion
 - Bestellung ist nach der DSGVO u.a. verpflichtend bei **Organisationen**, wenn ihre Kerntätigkeit
 - eine umfangreiche regelmäßige und systematische **Beobachtung** von betroffenen Personen erforderlich macht;
 - in der umfangreichen Verarbeitung **besonderer Kategorien von sensiblen Daten** oder Daten über strafrechtliche Verurteilungen und Straftaten.
 - Behörden und öffentliche Stellen müssen ebenfalls einen Datenschutzbeauftragten bestellen (Art 37 Abs 1 lit a DSGVO).
- **Aufgaben:** Unterrichtung/Beratung, Überwachung, Sensibilisierung, Schulung, Zusammenarbeit mit der Aufsichtsbehörde etc.

DSGVO – was haben Unternehmen zu beachten?

– Setzung technischer und organisatorischer Maßnahmen

- Zweck: Sicherstellung, dass Datenverarbeitung gemäß den Vorschriften der DSGVO erfolgt
- Maßnahmen sind auch **gegenüber der Aufsichtsbehörde nachzuweisen**
- organisatorische Maßnahmen:
 - interne Regelung für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten, für die Bestellung eines Datenschutzbeauftragten; System für den Umgang mit Zwischenfällen; Mitarbeiterschulungen; regelmäßige Kontrollen der Datenschutz-Compliance etc
- technische Maßnahmen:
 - „privacy by design“ (Datenschutz durch Technikgestaltung)
 - „privacy by default“ (Voreinstellungen)

DSGVO – was haben Unternehmen zu beachten?

– Informationspflichten

- dem Betroffenen sind durch den Verantwortlichen gewisse Informationen über die Datenanwendungen zur Verfügung zu stellen.
- Unterscheidung: Erhebung der Daten bei der betroffenen Person selbst / Erhebung der Daten bei anderen Personen
- Informationen müssen in **präziser, transparenter, verständlicher** und **leicht zugänglicher** Form in einer **klaren** und **einfachen Sprache** übermittelt werden.
- Übermittlung der Information erfolgt **schriftlich**, ggf. auch elektronisch oder mündlich (setzt Feststellung der Identität des Betroffenen voraus)
- Informationen können auch auf einer **Website** bereitgestellt werden, wenn sie für die Öffentlichkeit bestimmt sind (ErwG 58)

DSGVO – was haben Unternehmen zu beachten?

– Auskunftspflichten

- Betroffene hat **Auskunftsrecht** über seine **personenbezogenen Daten**
- große Menge an Informationen – Mitwirkungspflicht
- grsd **elektronisch**, außer betroffene Person wünscht eine andere Form
- Aushändigung der Kopie darf **nicht in die Rechte anderer Personen eingreifen**
- **unverzüglich** zu beantworten, in jedem Fall aber binnen eines Monats ab Eingang; bei **komplexen** Auskünften: **Verlängerung** um zwei Monate
- **erste Kopie** zwingend **unentgeltlich**; für weitere: angemessenes Entgelt
- bei Verletzung: Geldstrafen bis zu EUR 20 Mio oder 4% des weltweit erzielten Vorjahresumsatzes

Einsatz von Auftragsverarbeitern

- Verantwortliche kann für seine Verarbeitung Auftragsverarbeiter heranziehen
- **schriftlicher** Vertrag (Auftragsverarbeitervertrag) erforderlich
- Auftragsverarbeiter darf nur gemäß den **Weisungen** des Verantwortlichen tätig werden
- entscheidet Auftragsverarbeiter selbst über Verarbeitungszwecke- oder mittel
→ mutiert er bezüglich dieser Datenverarbeitung zum Verantwortlichen
- für Einsetzung von **Sub-Auftragsverarbeitern** ist **Zustimmung** des **Verantwortlichen** erforderlich und zwischen Auftragsverarbeiter und Sub-Auftragsverarbeiter ein **Vertrag** abzuschließen
- Vereinbarung, dass Auftragsverarbeiter nach Beendigung seiner Tätigkeit alle personenbezogenen Daten löscht oder zurück gibt, außer es besteht gesetzliche Pflicht zur Speicherung

Datenübermittlung an Drittländer

- innerhalb der EU keine Beschränkungen
- Übermittlung in Drittstaaten ist zulässig, wenn
 - 1. im Drittstaat ein **angemessenes Datenschutzniveau** besteht und dies die **Europäische Kommission** durch einen **Beschluss** festgestellt hat (derzeit: Andorra, Argentinien, die Färöer Inseln, Guernsey, die Isle of Man, Israel Jersey, Kanada Neu-seeland, die Schweiz Uruguay und USA (sofern Datenempfänger über eine **Privacy-Shield-Zertifizierung** verfügt)
 - 2. zwischen dem Übermittler (Verantwortlicher/Auftragsverarbeiter) und dem Empfänger **Standardvertragsklauseln** abgeschlossen wurden
- **Konzernverträge:** Daten dürfen innerhalb eines Konzerns in ein Drittland übermitteln werden, wenn der Konzern verbindliche Datenschutzvorschriften („**Binding Corporate Rules**“) implementiert hat, die von der Aufsichtsbehörde genehmigt wurden.

Datenübermittlung zwischen Konzerngesellschaften

- Erlaubnistatbestände für die Übermittlung von **Kundendaten**:
 - Notwendigkeit für die Erfüllung eines Vertrages,
 - überwiegend berechtigten Interessen des Verantwortlichen oder eines Dritten (Interessensabwägung),
 - Einwilligung des Betroffenen

- Erlaubnistatbestände für die Übermittlung von **Arbeitnehmerdaten**:
 - im Arbeitsverhältnis werfen die Erlaubnistatbestände „Einwilligung“ und „Notwendigkeit zur Erfüllung eines Vertrages“ erhebliche Probleme auf
 - insbesondere in Matrixorganisationen erkennt die Datenschutzbehörde grundsätzlich ein überwiegend berechtigtes Interesse an, dass Arbeitnehmerdaten an den Vorgesetzten einer anderen Konzerngesellschaft übermittelt werden.

- **Internationale Datenübermittlung im Konzern**
 - „Binding Corporate Rules“ (sehr aufwändiges Verfahren)
 - Standardvertragsklauseln

Besonderheiten des Arbeitnehmerdatenschutzes

- nach der DSGVO steht es den Mitgliedstaaten frei, durch nationales Recht, einschließlich durch Kollektivverträge und Betriebsvereinbarungen Sondervorschriften „zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext“ zu erlassen
- die in Ö bestehenden arbeitsrechtlichen Normen mit datenschutzrechtlichem Charakter werden auch nach dem Geltungsbereich der DSGVO anwendbar bleiben
- dies bedeutet insbesondere, dass in der Praxis nahezu alle Übermittlungen von **Arbeitnehmerdaten** in gesellschaftsrechtlichen Sachverhalten den **Abschluss einer Betriebsvereinbarung** voraussetzen

Ob in Betrieben ohne Betriebsrat die Zustimmung des Betriebsrates durch die Zustimmung der Arbeitnehmer ersetzt werden kann, ist strittig und eher zu verneinen.

Checkliste – Was ist zu tun?

- ✓ ist die DSGVO **anwendbar**? – sachlich, räumlich
- ✓ liegt eine **Datenverarbeitung** vor? Erfüllung der Grundsätze? Zweck der Datenverarbeitung? Erlaubnistatbestand?
- ✓ **Projektverantwortlichen** / Datenschutzbeauftragten bestellen
- ✓ **Compliance Check:** sorgfältige Prüfung und Dokumentation aller Datenverarbeitungen im Unternehmen; Status Quo erheben
- ✓ Erstellen und Führen eines **Verzeichnisses** aller Verarbeitungstätigkeiten
- ✓ Einrichtung **unternehmensinterne Prozesse** zur Erfüllung der Betroffenenrechte, Informationspflichten und Meldepflichten
- ✓ Umsetzung angemessener **Datensicherheitsmaßnahmen** (Datenschutz durch Technik und Voreinstellung)

Checkliste – Was ist zu tun?

- ✓ Grundprinzipien und Rechtsgrundlagen überprüfen; **Rechtmäßigkeit** (ev. Bestehende Einwilligungserklärungen / Verträge aktualisieren)
- ✓ Dienstleisterverträge abschließen
- ✓ Datenschutz-Folgenabschätzung
- ✓ interne Schulungen

Umsetzung der Datenschutz-Grundverordnung im Unternehmen

Mag. Michael Zeppelzauer, CISA, CIA

Einleitung

Strategie

Vorgehensmodell

Umsetzung im
Unternehmen

Datenschutz
Compliance

DSGVO – Risiko und Chance

→ Risiko

- Viele neue Bestimmungen für alle, geringe bis keine Erfahrungen mit den Behörden, aber auch geringe Erfahrung bei den Behörden selbst
- Viele unbestimmte Rechtsbegriffe wie zB „Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein“

→ Chancen

- Die Kunden wollen über die eigenen Daten bestimmen
- Datenschutz wird immer mehr zum Kaufkriterium
- Kunden überlegen immer genauer, wem sie vertrauliche Daten übergeben

→ **Datenschutz ist für uns alle, auch wir können „auf der anderen Seite sein“**

→ **Verabschieden wir uns von der Sammlermentalität!**

→ **Keine Verarbeitung – keine datenschutzrechtliche Behandlung notwendig**

Einleitung

Strategie

Vorgehensmodell

Umsetzung im
Unternehmen

Datenschutz
Compliance

Strategie/Ziele bei der Umsetzung der Anforderungen nach DSGVO

→ **Alle werden etwas tun müssen**

→ **Überlegungen**

- Konzernweite Strategie vs dezentraler Ansatz
- Offensive oder defensive Strategie im Umgang mit Daten
 - Wirtschaftlicher Nutzen aus den vorhandenen Daten oder reine „Verwaltungsdaten“
- Pragmatischer Ansatz versus sofortige 110%ige (Über-)Compliance
 - Eine sofortige vollinhaltliche Umsetzung der Anforderungen ist für die meisten Unternehmen nicht effizient
 - Die Interpretationen vieler Anforderungen sind noch nicht abgesichert – Durchsetzung einer „best practice“ bzw gerichtliche Entscheidungen bleiben abzuwarten
- Risikoorientierte Strategie bevorzugen
 - Prozesse sind wichtig („Wo liegt das Risiko im Unternehmen“)
 - Abhängig vom Unternehmensgegenstand Priorisierung auf Kunden-, Lieferanten- Dienstleister- oder Interner Datenverarbeitung

→ **Fokus auf Dokumentationspflichten**

Einleitung

Strategie

Vorgehensmodell

Umsetzung im
Unternehmen

Datenschutz
Compliance

Entwicklung eines Vorgehensmodells zur Vorbereitung auf die DSGVO

- Es sind nur noch wenige Tage bis zum Inkrafttreten der DSGVO
- Mit 25.5.2018 müssen alle Anforderungen umgesetzt sein UND der laufende Betrieb ab diesem Zeitpunkt reibungslos funktionieren
- Die Umsetzung im Unternehmen muss als Projekt definiert sein und die nötige Unterstützung des Managements haben (es ist KEIN EDV-Projekt)
- Mit Mitte Mai sollten alle „nach außen gerichteten Maßnahmen“ abgeschlossen sein um noch Zeit für eine abschließende Prüfung zu ermöglichen
- Projektressourcen sollten auch noch für den Rest von 2018 eingeplant werden, da erst im Rahmen der ersten Anforderungen und Entscheidungen der Datenschutzbehörde klar werden wird, welche Punkte noch zu bearbeiten sind bzw wie gewisse Bestimmungen ausgelegt sind

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Umsetzung im Unternehmen

- Management sensibilisieren
- Projekt aufsetzen
- Datenschutzorganisation im Unternehmen definieren
- Informationen über Prozesse erheben
- Verzeichnis der Verarbeitungstätigkeiten erstellen
- Rechtmäßigkeit der Verarbeitung prüfen
- Datenschutz-Folgeabschätzungen durchführen
- Unternehmensrichtlinien und Schulungen
- Datenschutz im laufenden Betrieb

Einleitung

Strategie

Vorgehensmodell

**Umsetzung im
Unternehmen**

Datenschutz
Compliance

Management sensibilisieren

→ **Motivation des Managements?**

- Reputationsschaden – Umsatzeinbußen
- Strafen für das Unternehmen
- Schadenersatzzahlungen
- Persönliche Folgen Positionsverlust bzw Haftung (im Regressfall)

→ **Datenschutz-Compliance**

- Es handelt sich um ein unternehmensweites Thema, nicht um ein reines IT-Thema
- Es beeinflusst die Organisation und die Prozesse nachhaltig und langfristig und muss bei zukünftigen Strategieentscheidungen berücksichtigt werden

→ **Umsetzung der Anforderungen**

- Personalressourcen werden gebunden
- Budget wird benötigt

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

DSGVO Umsetzungsprojekt aufsetzen

→ **Klassische Projektorganisation**

- Abhängig von Unternehmensgröße
- Ev Einbindung in Konzernprojekt
- Budgetrahmen definieren

→ **Fachliche Projektleitung**

- Meist im Bereich Recht oder Compliance angesiedelt

→ **Tools**

- Richtige Werkzeuge erleichtern die Arbeit
- Langfristig denken – Projekttools zur Erfassung sollten auch im laufenden Betrieb danach verwendbar sein.

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Datenschutzorganisation im Unternehmen definieren

→ **Wo liegt die Zuständigkeit im Unternehmen?**

- Rechtsabteilung, Compliance, Interne Revision, Organisation?

→ **Position Datenschutz-ManagerIn**

- Wer ist Datenschutz ManagerIn?
- Welche Aufgaben sind in dieser Position zu erledigen?
- (normalerweise zuständig für die „DSGVO-Compliance-Aufgaben“)
- Stellvertretung nicht vergessen

→ **Position Datenschutzbeauftragte/r**

- Aufgaben in der DSGVO geregelt
- Benötigt mein Unternehmen diese Funktion, wie wird die Unabhängigkeit sichergestellt?
- Datenschutz-ManagerIn und Datenschutzbeauftragte/r in einer Person?
- Auslagerung der Funktion/Konzerndatenschutzbeauftragte/r

→ **Weitere Zuständigkeiten**

- Konzerndatenschutzbeauftragter
- Datenschutzverantwortliche beim Auftragsverarbeiter
- Rechtsanwalt

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Information über Prozesse erheben

- **Prozesse im Unternehmen, bei denen Daten verarbeitet werden identifizieren und dokumentieren**
 - Vorhandene Prozessbeschreibungen müssen meist nur ergänzt werden
- **Zu erhebende Daten:**
 - Verantwortlicher für die Verarbeitung
 - Datenkategorien
 - Zweck der Verarbeitung
 - Auftragsverarbeiter (aktiv/passiv) und Vertragsgrundlage
 - Datenübermittlung an andere Verantwortliche (welche, an wen, warum, ...)
 - Grundlage für die Verarbeitung (zB Einwilligungserklärung)
 - Datensicherheitsmaßnahmen
- **Vorbedingung für das Verarbeitungsverzeichnis und die Prüfung auf Rechtmäßigkeit**

Einleitung

Strategie

Vorgehensmodell

**Umsetzung im
Unternehmen**

Datenschutz
Compliance

Verzeichnis der Verarbeitungstätigkeiten erstellen

- **Inhalt des Verzeichnisses in der DSGVO taxativ aufgezählt**
- **Idealerweise Erfassung in einem Tool**
- **Konzernverzeichnis vs Verzeichnis pro Niederlassung**
 - Klärung des Zugriffes für Behörden
 - Sprache
- **Abstimmung mit allfälligen Dienstleistern**

Einleitung

Strategie

Vorgehensmodell

**Umsetzung im
Unternehmen**

Datenschutz
Compliance

Rechtmäßigkeit der Verarbeitung prüfen

→ Für jede Verarbeitungstätigkeit muss geprüft werden

- Rechtsgrundlage vorhanden
- Zustimmungserklärungen ausreichend für die Verarbeitungstätigkeit
- Zustimmungserklärungen vorhanden?
- Datenschutzmitteilungen für Kunden korrekt gestaltet (alle Daten vorhanden)?
- Vereinbarungen mit Auftragsverarbeitern vollständig und unterzeichnet

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Datenschutz-Folgenabschätzung durchführen

➤ Schritt 1: Risikoeinschätzung

➤ Hintergrund

- Ersteinschätzung des Risikos der Datenverarbeitung hinsichtlich verarbeiteter Daten und deren Auswirkung, bei Verarbeitung sensibler Daten, Profiling oder Blacklist der Datenschutzbehörde → Datenschutz-Folgenabschätzung notwendig

➤ Unterstützung bei der Einschätzung

- Guideline der Artikel 29 Gruppe welche Punkte ein hohes Risiko signalisieren, treffen 2 Punkte zu → Datenschutz-Folgenabschätzung notwendig

➤ Schritt 2: Datenschutz-Folgenabschätzung (Data Privacy Impact Analysis)

- DPIA Frameworks bereits vorhanden (UK: ICO, F: CNIL, ISO 29134)
- ICO (UK) ist am besten praxisbezogen

➤ Ergibt die PIA ein hohes Risiko: Verpflichtende Konsultation der Datenschutzbehörde

➤ Bei der PIA sind Whitelist und Blacklist zu beachten (Whitelist in Österreich: fast alle Standardanwendungen abgedeckt)

Musterdokument des „Toolsets DSGVO“ der WKO Bundessparte Handel. Es gelten die Hinweise auf Seite 1!

www.kpra.at

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Technisch organisatorische Maßnahmen beurteilen/anpassen

→ **Definition Technisch Organisatorische Maßnahmen (Artikel 32)**

- Verantwortliche und Auftragsverarbeiter haben dafür zu sorgen, dass „**geeignete technische und organisatorische Maßnahmen**“ implementiert sind, die sicherstellen, dass „**ein dem Risiko angemessenes Schutzniveau gewährleistet ist**“

→ Maßnahmen:

- Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit der Systeme, rasche Wiederherstellung, Verfahren zur regelmäßigen Überprüfung, etc

→ **Für den Verantwortlichen zu berücksichtigen:**

- Stand der Technik
- Implementierungskosten
- Risiko (Eintrittswahrscheinlichkeit und Schwere des Risikos)

→ **Umsetzung im Unternehmen**

- Evaluierung der Maßnahmen, die unter „Allgemeine Computerkontrollen“ fallen und allenfalls Verbesserungsmaßnahmen
- IT-bezogenes Internes Kontrollsystem zur laufenden Bewertung dieser
- Bei Neuanschaffungen zu beachten: „privacy by design“, „privacy by default“

Einleitung

Strategie

Vorgehensmodell

Umsetzung im Unternehmen

Datenschutz
Compliance

Unternehmensrichtlinien und Schulungen

➤ **Richtlinien für Datenschutz Compliance erstellen**

- Allgemeine Richtlinie zum Umgang mit personenbezogenen Daten
- Richtlinie zur Informationssicherheit
- Richtlinie zum Umgang mit Datenschutzverletzungen (Data Breach Notification)

➤ **Bestehende Richtlinien überprüfen und ggfs anpassen**

- IT-Richtlinie
- Bring your own device Richtlinie
- Code of Ethics
- ...

➤ **Schulungen**

- Verpflichtende Schulungen einführen
- Allgemeine Schulungen und für die jeweiligen Arbeitsgebiete (siehe Richtlinien)
- Dokumentation des Schulungsbesuchs

Einleitung

Strategie

Vorgehensmodell

Umsetzung im
Unternehmen

**Datenschutz
Compliance**

Datenschutz im laufenden Betrieb

- **Datenschutz ist eine laufende Compliance-Maßnahme**
- **Datenschutz muss im täglichen Betrieb aufrechterhalten werden**
 - Position des Datenschutz-Managers und des Datenschutzbeauftragten
 - Beantwortung von Fragen von Betroffenen
 - Erfassung neuer bzw geänderter Verarbeitungstätigkeiten
 - Reaktion auf Zwischenfälle
 - Laufendes Reporting an das Management
 - Laufende methodische Weiterentwicklung bei geänderten gesetzlichen Vorgaben oder Entscheidungen
 - Periodische Überprüfung durch die Interne Revision
 - Periodische Abhaltung von Schulungen

Einleitung

Strategie

Vorgehensmodell

Umsetzung im
Unternehmen

**Datenschutz
Compliance**

Gelebter Datenschutz vs Datenschutz am Papier

- **Datenschutz wird ein Kaufkriterium**
- **Die mündigen Bürger wollen über ihre eigenen Daten selbst bestimmen**
- **Datenschutz im Unternehmen**
 - Daten und Digitalisierung sind die neue „industrielle“ Revolution
 - Der Wert von Daten wird immer weiter bekannt
 - Daten und damit einhergehend Datenschutz werden für den Unternehmenserfolg immer wichtiger
 - Datenschutz ist mehr wie eine reine „neue“ Compliance Richtlinie
 - Risikoorientierte Umsetzung

curriculum vitae



Mag. Mario Schmieder

Mario Schmieder ist Rechtsanwalt und seit 2006 Partner bei Kerschbaum Partner Rechtsanwälte. Der Fokus seiner Arbeit liegt in der Vertretung seiner Mandanten in allen wirtschafts- und finanzstrafrechtlichen Fragen. Ebenso berät er diese umfassend im Bereich Compliance.

Vor seiner Tätigkeit bei Kerschbaum Partner Rechtsanwälte war Mario Schmieder unter anderem als selbständiger Rechtsanwalt sowie bei einem Big Four Unternehmen beschäftigt.

Mario Schmieder publiziert und referiert regelmäßig zu seinen Schwerpunkten. Darüber hinaus ist er Mitherausgeber der ZWF (Zeitschrift für Wirtschafts- und Finanzstrafrecht).

Rechtsanwalt | Partner

t +43 732 73 03 69-110

e mario.schmieder@kpra.at

curriculum vitae



Cert. Internal Auditor |
Cert. Information
Systems Auditor |
Manager
t +43 1 718 98 90-462
e michael.zeppelzauer@
leitnerleitner.com

Mag. Michael Zeppelzauer, CIA, CISA

Michael Zeppelzauer ist Certified Internal Auditor, Certified Information Systems Auditor und zertifizierter Quality Assessor. Er ist seit 2017 als Manager bei LeitnerLeitner tätig. Davor hat er bei einer Big Four Kanzlei 11 Jahre lang den Bereich Assurance Services (Interne Revision, Risikomanagement, etc) aufgebaut und geleitet und in der Folge war er 8 Jahre lang Konzernrevisionsleiter der bauMax AG mit der Verantwortung für Risikomanagement und Compliance. Im Rahmen des Wind Downs war er Co-Projektleiter. Daneben war er als Quality Assessor bei öffentlichen Unternehmen tätig.

Seine Tätigkeitsschwerpunkte liegen in den Bereichen Assurance Services mit den Schwerpunkten Compliance (inkl Datenschutz), Interne Revision, Risikomanagement, Datenanalyse und EDV-Systemprüfung. Darüber hinaus ist Michael Zeppelzauer Mitglied im Fachsenat für Datenverarbeitung der Kammer der Wirtschaftstrehänder und Mitautor an Fachpublikationen (zB „Interne Revision - Gestaltung und Organisation in der Praxis“).

beograd
bratislava
budapest
linz
ljubljana
praha
salzburg
sarajevo
wien
zagreb
zürich
praha *
sofia *

* kooperation



LeitnerLeitner Consulting d.o.o.

SRB 11000 BEOGRAD, Knez Mihailova Street 1-3
t +381 11 655 51 05 f +381 11 655 51 06
e office.belgrade@leitnerleitner.com

BMB Leitner k.s.

SK 811 01 BRATISLAVA, Zámocká 32
t +421 2 591 018-00 f +421 2 591 018-50
e bratislava.office@bmbleitner.sk

LeitnerLeitner CZ, s.r.o.

CZ 180 00 PRAHA 8, Voctářova 5
t +420 22 888 3900
e office.prague@leitnerleitner.cz

Leitner + Leitner Tax Kft

H 1027 BUDAPEST, Kapás utca 6-12
t +36 1 279 29-30 f +36 1 209 48-74
e office@leitnerleitner.hu

LeitnerLeitner GmbH

Wirtschaftsprüfer und Steuerberater
A 4040 LINZ, Ottensheimer Straße 32
t +43 732 70 93-0 f +43 732 70 93-156
e linz.office@leitnerleitner.com

Leitner + Leitner d.o.o.

SI 1000 LJUBLJANA, Dunajska cesta 159
t +386 1 563 67-50 f +386 1 563 67-89
e office@leitnerleitner.si

LeitnerLeitner Salzburg GmbH

Wirtschaftsprüfer und Steuerberater
A 5020 SALZBURG, Hellbrunner Straße 7
t +43 662 847 093-0 f +43 662 847 093-825
e salzburg.office@leitnerleitner.com

Leitner + Leitner Revizija d.o.o.

BIH 71 000 SARAJEVO, Ul. Hiseta 15
t +387 33 465-793
e office@leitnerleitner.ba

LeitnerLeitner GmbH

Wirtschaftsprüfer und Steuerberater
A 1030 WIEN, Am Heumarkt 7
t +43 1 718 98 90 f +43 1 718 98 90-804
e wien.office@leitnerleitner.com

LeitnerLeitner Consulting d.o.o.

HR 10 000 ZAGREB, Heinzelova ulica 70
t +385 1 60 64-400 f +385 1 60 64-411
e office@leitnerleitner.hr

LeitnerLeitner Zürich AG

CH 8001 ZÜRICH, Bahnhofstrasse 69a
t +41 44 226 36 10 f +41 44 226 36 19
e zuerich.office@leitnerleitner.com

kooperationen

Fučík & partneři, s.r.o.

CZ 110 00 PRAHA 1, Klimentská 1207/10
t +420 296 578 300 f +420 296 578 301
e ff@fucik.cz

Tascheva & Partner

BG 1303 SOFIA, Ulitsa Marko Balabanov 4
t +359 2 939 89 60 f +359 2 981 75 93
e office@tashevapartner.com