Umsetzung der Anforderungen nach Datenschutz-Grundverordnung in Handelsunternehmen – „Toolset DSGVO“

Mag. Michael Zeppelzauer, CISA, CIA

Linz, 7. März 2018

Mag. Michael Zeppelzauer - LeitnerLeitner

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

Mag. Michael Zeppelzauer

- *Seit 2017 Manager bei LeitnerLeitner in Wien im Bereich Assurance Services (Compliance, Interne Revision, IT-Prüfung etc)*
- *Von 2008 bis 2016 Internationaler Konzernrevisionsleiter bauMax (inkl Sicherheitsagenden und Compliance)*
- *Davor mehr wie 10 Jahre Deloitte Enterprise Risk Services*
- *Zertifizierter Datenschutzbeauftragter, Certified Internal Auditor, Certified Information Systems Auditor*

LeitnerLeitner

- *LeitnerLeitner ist eine der maßgebenden Sozietäten von Wirtschaftsprüfern und Steuerberatern in Österreich, Zentral- und Osteuropa. Hinter jedem persönlichen Ansprechpartner stehen rund 750 Mitarbeiter und weltweite Kooperationspartner für die Beratung sowohl mittelständischer Unternehmen als auch Konzerne*

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!**

Strategie/Ziele bei der Umsetzung der Anforderungen nach DSGVO

- **Alle werden etwas tun müssen**

- **Überlegungen**
  - 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 – „Toolset DSGVO“**

Notwendigkeit der Entwicklung eines Vorgehensmodells zur Vorbereitung auf die DSGVO im Unternehmen

- Es sind ab 7.3.2018 noch 80 Tage Inkrafttreten der Maßnahmen nach DSGVO
- Mit dem 25.5.2018 müssen alle Anforderungen umgesetzt sein UND der laufende Betrieb ab diesem Zeitpunkt reibungslauf funktionieren
- Vorgehensmodell mit Projektschritten ist notwendig um die Umsetzung rechtzeitig zu schaffen.

- **Unterstützung durch das „Toolset DSGVO" der Bundessparte Handel der WKO**

- Aber für jedes Unternehmen ist folgendes zu beachten:
  - Das Toolset DSGVO der WKO Bundessparte Handel ist als Standardmodell zur Unterstützung gedacht, muss aber an das Unternehmen angepasst werden.
  - Es ist nur das Datenschutzrecht inbegriffen, alle anderen Rechtsvorschriften werden nicht berücksichtigt
  - Die Umsetzung im Unternehmen muss als Projekt definiert sein und die nötige Unterstützung des Managements haben (es ist KEIN EDV-Projekt).
  - Projektressourcen sollten auch noch für den Rest von 2018 eingeplant werden, da erst im Rahmen der ersten Entscheidungen der Datenschutzbehörde Klarstellung zu manchen Punkten erfolgen wird.

Schritte zur Umsetzung der Anforderungen nach DSGVO im Unternehmen

- Management sensibilisieren
- Projekt aufsetzen
- Datenschutzorganisation im Unternehmen definieren
- Informationen über Prozesse erheben und Verzeichnis der Verarbeitungstätigkeiten erstellen
- Rechtmäßigkeit der Verarbeitung prüfen
- Rechtskonformität der Auftragsverarbeitung sicherstellen
- Technisch organisatorische Maßnahmen beurteilen/anpassen
- Datenschutz-Folgeabschätzungen durchführen
- Unternehmensrichtlinien und Schulungen
- Datenschutz im laufenden Betrieb

- Diese Schritte zur Umsetzung werden durch das „Toolset DSGVO der WKO Bundessparte Handel unterstützt.

Management sensibilisieren

- **Motivation des Managements?**
  - Reputationsschaden – Umsatzeinbußen
  - Strafen für das Unternehmen (verhängt durch die Datenschutzkommission)
  - Schadenersatzzahlungen (verhängt durch Gerichte)
  - 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

- Präsentation „Einführung in den Datenschutz neu“

DSGVO Umsetzungsprojekt aufsetzen

- **Klassische Projektorganisation**
  - Abhängig von Unternehmensgröße
  - Eventuell Einbindung in Konzernprojekt
  - Budgetrahmen definieren

- **Fachliche Projektleitung**
  - Bei Kleinbetrieben meist die Geschäftsführung
  - Bei großen Unternehmen meist im Bereich Recht oder Compliance angesiedelt
  - Ev externe Unterstützung

- **Tools**
  - Richtige Werkzeuge erleichtern die Arbeit
  - Langfristig denken – Tools sollten auch im laufenden Betrieb danach verwendbar sein

- Erläuterung Toolset
- Beispielprojektplan

Datenschutzorganisation im Unternehmen definieren

- **Wo liegt die Zuständigkeit im Unternehmen?**
  - Geschäftsführung, Rechtsabteilung, Compliance, Interne Revision, Organisation?

- **Position Datenschutz-ManagerIn (Verantwortliche/r)**
  - Wer ist Datenschutz ManagerIn?
  - Welche Aufgaben sind in dieser Position zu erledigen?
  - normalerweise zuständig für die „DSGVO-Compliance-Aufgaben"

- **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 an externe Firma oder Konzerndatenschutzbeauftragte/r?

- Definition DatenschutzmanagerIn/Verantworliche/r
- Datenschutzorganisation im Unternehmen
- Entscheidungsbaum Datenschutzbeauftragte/r

Information über Prozesse erheben und Verzeichnis der Verarbeitungstätigkeiten

- **Prozesse im Unternehmen, bei denen Daten verarbeitet werden identifizieren und dokumentieren**
  - Vorhandene Prozessbeschreibungen müssen meist nur ergänzt werden
  - Möglichst nur Standardprozesse, alles andere „einstellen" oder extra dokumentieren

- **Verzeichnis der Verarbeitungstätigkeiten erstellen**
  - Inhalt des Verzeichnisses in Artikel 30 taxativ aufgezählt
  - Idealerweise Erfassung in einem Tool
  - Konzernverzeichnis vs Verzeichnis pro Niederlassung
  - Abstimmung mit allfälligen Dienstleistern
  - Vergleich mit dem derzeitigen DV-Register (ua auch den Standardanwendungen)
  - Besonderheit der Online-Shops

- **Vorbedingung für das Verarbeitungsverzeichnis und die Prüfung auf Rechtmäßigkeit**

- Musterverzeichnis nach Standardverordnungen
- Musterdatenschutzerklärung für Website
- Erläuterung zu Onlineshops

Rechtmäßigkeit der Verarbeitung prüfen

- **Für jede Verarbeitungstätigkeit muss geprüft werden**

- **Rechtsgrundlage vorhanden**
  - Bei Einwilligung:
    - Zustimmungserklärungen ausreichend für die Verarbeitungstätigkeit?
    - Zustimmungserklärungen vorhanden?

- **EXKURS:**
  - Eintragung in Mailinglisten
  - Abmeldung von Mailinglisten

- **Datenschutzmitteilungen für Kunden korrekt gestaltet (alle Daten vorhanden)?**
  - Mitteilung auf der Website

- **Vereinbarungen mit allfälligen Auftragsverarbeitern vollständig und unterzeichnet?**

- Aufzählung Rechtsgrundlagen der Verarbeitung
- Entscheidungsbaum Videoüberwachung
- Umgang mit Interessentendaten (Mailinglisten)

Rechtskonformität der Auftragsverarbeitung sicherstellen

- **Schriftliche Vereinbarungen mit Auftragsverarbeitern mit den Inhalten gemäß Artikel 28 DSGVO**
  - Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen (inkl Informationspflicht bei abweichender rechtlicher Verpflichtung)
  - Vertraulichkeitserklärung/Verschwiegenheitspflicht des Personals
  - Sicherstellung von technischen und organisatorischen Datenschutzmaßnahmen
  - Zustimmungsrechte oder Informationspflicht mit Einspruchsrecht bei Subauftragsverarbeitern und Überbindung aller eigenen Verpflichtungen
  - Verpflichtung zur Unterstützung des Verantwortlichen hinsichtlich Datensicherheit und Betroffenenrechte
  - Pflicht zur Datenlöschung/-rückgabe nach Beendigung der Tätigkeit
  - Nachweis- und Inspektionsrechte

- **Rechenschaftspflicht des Verantwortlichen über die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter (Auswahlverschulden)**

- Beispiel Auftragsverarbeitungsvertrag (Mustervertrag)

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"

- Beschreibung von notwendigen Maßnahmen

Datenschutz-Folgenabschätzung durchführen

- **Notwendig bei der Verarbeitung sensibler Daten**

- **1. Schritt: 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

- **Datenschutz-Folgenabschätzung (Data Privacy Impact Analysis)**
  - DPIA Frameworks bereits vorhanden (UK: ICO, F: CNIL, ISO 29134)
  - ICO (UK) - hat den größten Praxisbezug

- **Ergibt die Folgenabschätzung (PIA) ein hohes Risiko: Verpflichtende Konsultation der Datenschutzbehörde**

- Risikoeinschätzung (Ergebnis im Muster: kein Risiko)

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 gegebenenfalls anpassen**
  - IT-Richtlinie
  - Code of Ethics
  - …

- **Schulungen**
  - Verpflichtende Schulungen einführen
  - Dokumentation des Schulungsbesuchs

- Richtlinie Datenschutz im Unternehmen
- Richtlinie Umgang mit vertraulichen Daten
- Richtlinie Umgang mit Datenträgern
- Schulungsunterlage und -dokumentation

Datenschutz im laufenden Betrieb

- **Datenschutz ist eine laufende 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

- Prozess Datenschutzanfrage inkl Aushang
- Prozess/Richtlinie Data Breach
- Logbuch Datenschutz
- Prozess Anfragen Datenschutzkommission

Unterstützung bei der Umsetzung in der Praxis „Toolset DSGVO" der WKÖ Bundessparte Handel

- **Anforderungen an Unternehmen sind ähnlich**
  - Unternehmen der gleichen Branche haben ähnliche Anforderungen
  - Standardisierung ist möglich (wie auch schon im Datenverarbeitungsregister)
- **Dokumentation ist wichtig**
  - Der Nachweis der getroffenen Maßnahmen wird immer wichtiger
- **Standardabläufe**
  - Bringen Kostenreduktion für den Einzelnen
  - Reduktion des Risikos
  - Vollständigkeit der Dokumentation

- **„Toolset DSGVO" Fertigstellung Ende 01/2018**

- **Umsetzungspaket für Standardabläufe im Handel**
- **Individuelle Anpassung an das Unternehmen notwendig**
- **Beschäftigung mit Datenschutz notwendig**

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 Wirtschaftstreuhänder und Mitautor an Fachpublikationen (zB „Interne Revision - Gestaltung und Organisation in der Praxis“).

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

* 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 120 00 PRAHA, Římská 12
t +420 773 511 879 t +421 903 482 702
e office@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

Stalfort Legal. Tax. Audit.
RO 012083 BUCUREŞTI, Str. Lt. Av. Vasile Fuica Nr. 15
t +40 21 301 03 53 f +40 21 315 78 36
e bukarest@stalfort.ro

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@taschevapartner.com

MDDP
PL 00-542 WARSZAWA, 49 Mokotowska Street
t +48 22 322 68 88 f +48 22 322 68 89
e biuro@mddp.pl