cyberlegal

# Praxisleitfaden zur Datenschutz-Grundverordnung (EU-DSGVO) aus Compliance-Sicht

von RA Robert Niedermeier (Cyberlegal Rechtsanwälte),
RAin Petra Gummermann (Cyberlegal Rechtsanwälte)
und RAin Dorothea Teichmann (Cyberlegal Rechtsanwälte)

**In Zusammenarbeit mit**

ROHDE&SCHWARZ
Cybersecurity

eicar
EXPERT GROUP FOR IT-SECURITY

## Kontaktieren Sie uns

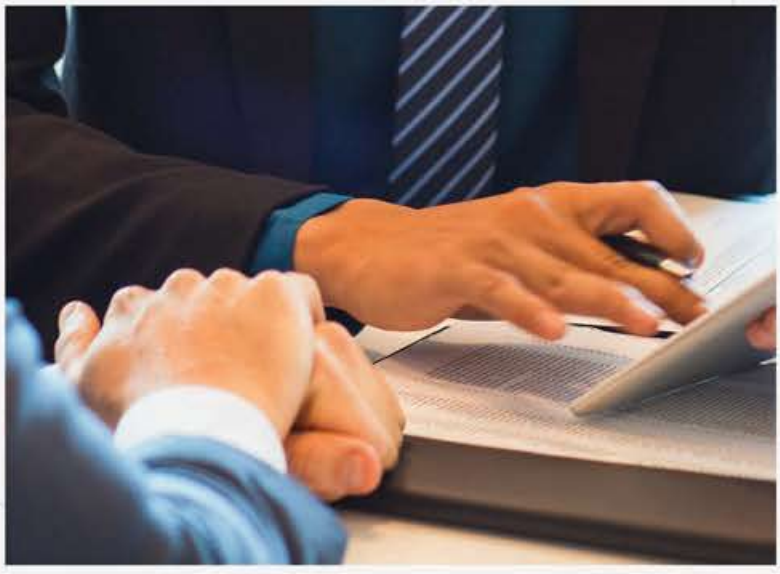
**Rohde & Schwarz Cybersecurity GmbH**
Mühldorfstraße 15
81671 München

+49 30 65884-223

cybersecurity@rohde-schwarz.com

www.cybersecurity.rohde-schwarz.com

# Vorwort



Die europäische Datenschutzgrundverordnung (DSGVO) ist ein seit Monaten viel diskutiertes Thema im IT-Sicherheitsumfeld, schließlich muss sie bis Mai 2018 umgesetzt werden. Sie gilt weltweit für alle Unternehmen, welche Daten von EU-Bürgern verarbeiten und speichern. Sie bedeutet eine Verschiebung der Rechtsprechung aus dem Zivilrecht ins Strafrecht sowie eine signifikante Erhöhung der Bußgelder bei Verstößen im mehrstelligen Millionenbereich. Durch diese beiden Faktoren – Haftbarkeit und finanzieller Verlust – schafft die DSGVO die nötige Sensibilisierung für Datenschutz auf den Unternehmensebenen.

An konkretem Tatendrang mangelt es trotzdem vielerorts in den Chefetagen. Wahrscheinlich, weil mit dem „Stand der Technik“ die konkreten technischen und organisatorischen Vorgaben der DSGVO nicht eindeutig geklärt und dadurch durchaus auslegungsfähig sind. Vielleicht auch, weil es schwer ist, einen Überblick über die gespeicherten Daten in zahlreichen IT-Systemen zu bekommen.

Welches Technologielevel ist angemessen für welche Unternehmen, Branchen und Geschäftsmodelle? Es bleibt den Gerichten überlassen, wie die Brücke zwischen entfernt bedrohlicher Theorie und konkret schmerzhafter Realität geschlagen wird.

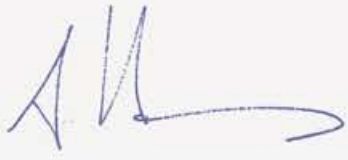
Wegen der weitgehend allgemeingültigen Natur der Verordnung wird es in absehbarer Zeit einen Präzedenzfall geben. Für Unternehmen, die bis dahin keine Maßnahmen zur Implementierung der DSGVO ergriffen haben, werden die möglichen Schäden umso schwerer ausfallen. Daher ist es entscheidend, keine Zeit mehr zu verlieren und mit einem erfahrenen und kompetenten Partner den Reifegrad der eigenen IT-Security unter die Lupe zu nehmen.

Die technischen Vorgaben sind dabei nicht alles. Auch organisatorisch wird mit der DSGVO ein gehöriger Ruck durch die Abteilungen gehen. Wer ist verantwortlich für die Umsetzung all der neuen Anforderungen und Richtlinien? Wer ist haftbar? Und wo fange ich am besten an?

Um diese Fragen zu beantworten, haben wir gemeinsam mit IT-Rechtsexperten diesen Compliance-Leitfaden zusammengestellt. Er bietet Ihnen praxisnahe und umsetzbare Tipps, um die Herausforderungen der DSGVO in Chancen umzuwandeln. Dieser Leitfaden kann Ihnen als Anhang Ihrer Unternehmensregeln dienen und stellt somit ein praktikables Werkzeug im Umgang mit den neuen Gesetzmäßigkeiten dar.

In der konkreten Umsetzung bieten wir Workshops zur Analyse des Ist-Standes, Beratung und Konzepte für die Planung und Durchführung von internen Projekten zur Compliance und gegebenenfalls begleitende Einführung eines Informationssicherheitsmanagementsystems (ISMS) sowie konkrete Lösungen für den Einsatz und Betrieb DSGVO-konformer Anwendungs- und Infrastrukturkomponenten an.

Dr. Alexander Schellong
Global Vice President Solutions & Services
Rohde & Schwarz Cybersecurity GmbH



Helko Kögel
Director Consulting
Rohde & Schwarz Cybersecurity GmbH

# INHALTSVERZEICHNIS


A. Einleitung ---------- 6

B. Compliance und Datenschutz ---------- 6

I. Compliance 6

II. Verantwortlichkeit /(Verantwortliche) Personen für den Datenschutz im Unternehmen 6

1. Geschäftsführung 6

2. IT-Leitung 7

III. Allgemeine rechtliche Überlegungen/Rechtsgrundlagen 9

1. EU-DSGVO und BDSG-neu 9

2. IT-Sicherheitsgesetz bei Sektorunternehmen 9

3. Datenschutzfolgenabschätzung 10

4. Betrieblicher Datenschutzbeauftragter 10

5. Auftragsdatenverarbeitung (innerhalb/außerhalb EU) 11

6. Dokumentationspflichten 12

7. Haftungsfragen 13

a) Zivilrechtliche Haftung

b) Strafrechtliche Haftung

C. Welche Datenschutzprozesse müssen im Unternehmen bestehen? ---------- 14

I. Dokumentation der Datenverarbeitungsprozesse im Unternehmen 14

II. Erweiterung der Informationspflichten Art. 14 DSVGO – Dokumentation von Datenschutzerklärungen 15

III. Prozess zur Abgabe und Widerruf von Einwilligungserklärungen 16

IV. Dokumentation des Verfahrens zur Portabilität 16

V. Anpassung bestehender Betriebsvereinbarungen an EU-DSGVO 16

VI. Nachweis der Vereinbarungen zur Auftragsverarbeitung 17

VII. IT-Sicherheitsprüfung 18

VIII. Schulungen zur EU-DSGVO und bestehenden eigenen Prozessen des internen Datenschutzkonzepts 18

IX. Datenpannen – erweiterte Obliegenheiten 19

D. Backdoor-freie Software ---------- 20

E. EU-DSGVO – möglicher Fahrplan eines EU-DSGVO Projekts: ---------- 21

F. Checkliste ---------- 23

# A Einleitung

Seit 25. Mai 2016 ist die Europäische Verordnung zum Datenschutz (Datenschutzgrundverordnung = EU-DSGVO) in Kraft und nach Ablauf der Übergangsfrist am 25. Mai 2018 wird sie auch durchgesetzt. Die EU-DSGVO soll das europäische Datenschutzrecht vereinheitlichen und die Durchsetzung dieses Rechts verbessern. Darüber hinaus enthält sie einige Neuerungen zur bis dahin geltenden Richtlinie 95/46/EG (Datenschutzrichtlinie) von 1995. Daher wird im Folgenden kurz dargestellt was aus Praxissicht für Unternehmen nun zu beachten ist und was bis Mai 2018 noch getan werden sollte.

# B Compliance und Datenschutz

## I. Compliance

Der Begriff „Compliance" umfasst grundsätzlich die Vereinbarkeit aller Unternehmenshandlungen mit geltenden gesetzlichen Vorschriften. Das beinhaltet logischerweise auch die Einhaltung der datenschutzrechtlichen Vorgaben. Im Einzelnen bedeutet dies für Unternehmen die Implementierung komplexer Prozesse und Festlegungen eindeutiger Verantwortlichkeiten entweder innerhalb der bestehenden Struktur oder durch den Einbezug externer Fachkräfte.

## II. Verantwortlichkeit /(Verantwortliche) Personen für den Datenschutz im Unternehmen

### 1. Geschäftsführung

Für den Datenschutz im Unternehmen ist nach der Datenschutzgrundverordnung primär der Geschäftsführer bzw. Vorstand **direkt verantwortlich**. Dies ergibt sich zwangsläufig aus den Haftungsregelungen, die eine persönliche Haftung des Geschäftsführers bzw. Vorstands vorsehen. Die Haftung erstreckt sich dabei sowohl auf das Privatvermögen als auch auf die persönliche Strafbarkeit, also die Gefahr einer Haftstrafe.

**Datenschutz wird also Chefsache!**

Ebenso verantwortlich ist der Datenschutzbeauftrage des Unternehmens. Ein solcher sollte, soweit noch nicht erfolgt, zeitnah durch die Geschäftsführung bestellt werden.
Ob es sich dabei um einen internen oder externen Datenschutzbeauftragten handelt, ist jedem Unternehmen selbst überlassen.

## 2. IT-Leitung

Die Geschäftsleitung kann unter anderem die IT-Leitung mit der tatsächlichen Umsetzung der Datenschutzgrundverordnung beauftragen. Teil der Informationssicherheit ist der Datenschutz und die Datensicherheit, die sich jeweils teilweise überschneiden.

Ein **Informationssicherheitskonzept,** das sich an dem Stand der Technik ausrichtet, ist hierbei das gesetzliche Anforderungsprofil. Die IT-Leitung hat bei der Implementierung des Informationssicherheitskonzepts daher die EU-DSGVO, das Bundesdatenschutzgesetz in seiner neuen Fassung (BDSG-neu; [1]), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG; [2]), Eigenkapitalvorschriften (sogenannte BASEL III Vorschriften; [3]), das IT-Sicherheitsgesetz und weitere branchenspezifische Spezialgesetze die Informationssicherheit betreffend zu berücksichtigen.

Ein solches IT-Sicherheitskonzept kann aus verschiedenen Gründen zwingend erforderlich sein.
Es kann gesetzlich vorgeschrieben sein ein IT-Sicherheitskonzept zu haben, dies ist beispielsweise für Sektorunternehmen der Fall. Regelungen können sich aus §§ 91 Abs. 2, 93 Abs. 2 AktG, § 43 Abs. 1 HGB, § 317 IV HGB, § 11 I a-c EnWG aber auch aus dem TKG, BSIG und der BSI-KritiS Verordnung.
Die Notwendigkeit eines IT-Sicherheitskonzepts kann sich aber auch aus anderen Faktoren ergeben, beispielsweise um den Schutz eigener Entwicklungen, interner Informationen, Mitarbeiterdaten, wettbewerbsrelevanter Informationen etc. nachweisbar und strukturiert sicherzustellen. Auch Compliance oder Haftungsrisiken sind Gründe für ein IT-Sicherheitskonzept.

1. https://dsgvo-gesetz.de/bdsg-neu/
2. https://www.bgbl.de
3. http://www.bundesbank.de

Mögliche Standards für ein IT-Sicherheitskonzept können die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sein. Es bietet sich auch die Zertifizierung des IT-Sicherheitskonzepts nach ISO 27001 an. Eine Zertifizierung kann vielfältige Vorteile haben, wie höheres Kundenvertrauen, geringere Versicherungsbeiträge und die Erfüllung international anerkannter Anforderungen.

Teil des Informationssicherheitskonzepts ist die Definition geeigneter Administratoren und deren Zuständigkeiten. Die EU-DSGVO verpflichtet alle Unternehmen, aufgrund der bestehenden Dokumentationspflichten geeignete Rollenkonzepte, insbesondere auch für Rollen der Administratoren, nachzuweisen.

Teil der Verantwortlichkeit von Administratoren im Rahmen des bestehenden Informationssicherheitskonzepts kann z.B. auch die **Prüfung der bestehenden Rollenkonzepte einzelner im Unternehmen verwendeter Softwareanwendungen, die personenbezogene Daten verarbeiten** auf die Einhaltung der EU-DSGVO-Grundsätze sein.

Sofern im Unternehmen bestehend sollten Chief Information Security Officer (CISO) als Verantwortlicher für Informationssicherheit in einer Organisation und der Datenschutzbeauftragte (DSB) die Einführung und Umsetzung der EU-DSGVO als Gemeinschaftsaufgabe realisieren und mit ihrem Fachwissen und Informationen das Schließen bestehender Lücken sicherstellen. Hierzu wird ggf. eine Zusammenarbeit im Rahmen eines EU-DSGVO Projekts notwendig.

Die Einzelaufgaben des CISO wie beispielsweise

- Erarbeitung und Definition der sicherheitsrelevanten Objekte, der Bedrohungen und Risiken und den daraus abgeleiteten Sicherheitszielen
- Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele
- Ausarbeitung, Anpassung von Sicherheitsrichtlinien
- Auditierung der Funktionseinheiten zum Stand der Umsetzung und Weiterentwicklung der Sicherheitsvorschriften
- Bewusstsein der Mitarbeiter durch Trainings und Kampagnen schaffen

ergänzen hierbei inhaltlich maßgeblich die Prüfungspunkte des Datenschutzbeauftragten zu Einhaltung der EU-DSGVO.

# III. Allgemeine rechtliche Überlegungen/Rechtsgrundlagen

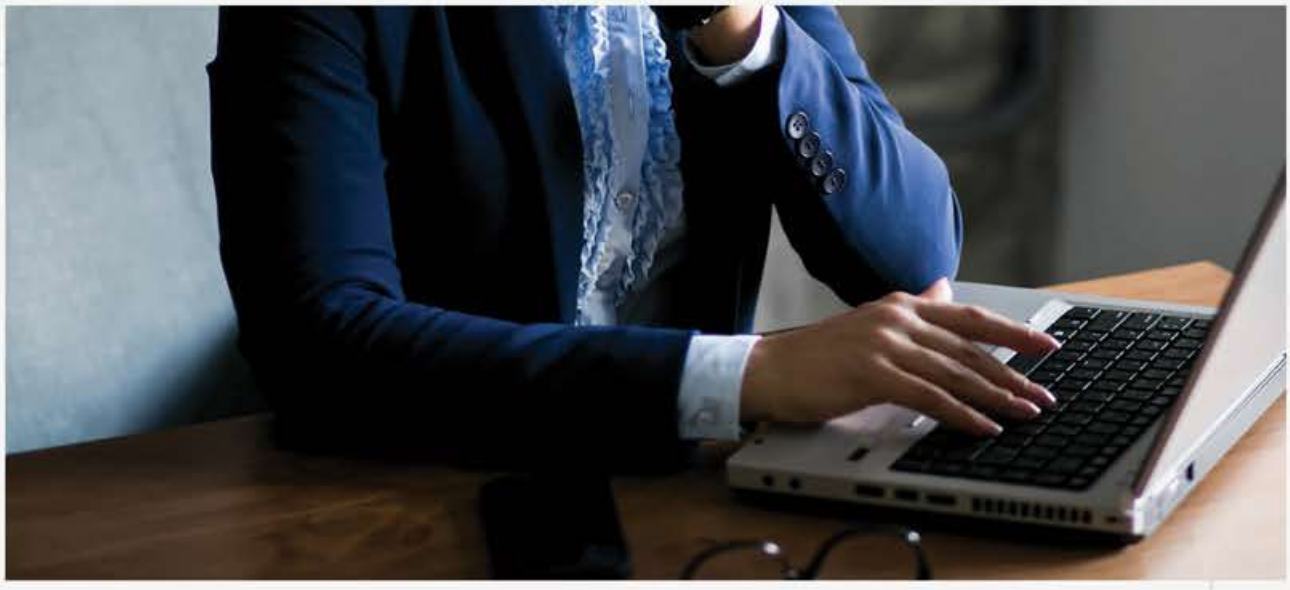
Der Datenschutz erhält ab 25. Mai 2018 eine neue Rechtsgrundlage. Das bisherige BDSG wird durch die Datenschutzgrundverordnung und das neue BDSG abgelöst.

## 1. EU-DSGVO und BDSG-neu

Die EU-DSGVO regelt den Datenschutz umfassend. Sie ist eine europäische Verordnung und als solche unmittelbar geltendes Recht in allen EU-Mitgliedstaaten. Das hat den Vorteil, dass Datenschutz in der EU nun weitestgehend einheitlichen Regeln folgt.

Warum also auch ein neues BDSG?
Die EU-DSGVO enthält an einigen Stellen Öffnungs- und Anpassungsklauseln, die den nationalen Gesetzgeber berechtigen, eigene Gesetze hierzu zu erlassen, von denen der deutsche Gesetzgeber Gebrauch gemacht hat. Das BDSG wurde in einem umfassenden Prozess an die EU-DSGVO angepasst und die Möglichkeiten der Öffnungsklausel wurden genutzt. Eine dieser Öffnungsklauseln betrifft die Pflicht zur Bestellung des Datenschutzbeauftragten. Das BDSG-neu wird wie bisher auch eine Pflicht zur Bestellung des Datenschutzbeauftragen bei mindestens 10 Personen, die mit der automatisierten Verarbeitung personenbezogener Daten betraut sind, regeln. Damit wird die Regelung der EU-DSGVO durch eine anspruchsvollere auf nationaler, deutscher Ebene ersetzt.

Dennoch hat in Zweifelsfällen die EU-DSGVO Vorrang vor dem neuen BDSG.
Vorlagen zur Überprüfung des BDSG-neu beim europäischen Gerichtshof (EuGH) zur Überprüfung der Vereinbarkeit des BDSG-neu mit der EU-DSGVO werden für einige Regelungen des BDSG-neu erwartet.



## 2. IT-Sicherheitsgesetz bei Sektorunternehmen

Für Unternehmen die im Bereich der kritischen Infrastrukturen (KRITIS) wie zum Beispiel Strom- und Wasserversorgung, Finanzen und Ernährung tätig sind, gelten für IT-Anlagen noch die zusätzlichen Anforderungen des IT-Sicherheitsgesetztes.[1]

1. http://www.bmi.bund.de/DE/Veroeffentlichungen/GesetzeVerordnungen/gesetzeverordnungen_node.html

## 3. Datenschutzfolgenabschätzung

Neu ist die Datenschutzfolgenabschätzung in Art. 35 EU-DSGVO. Das ist eine Vorprüfung von Verarbeitungsvorgängen, die ein hohes Risiko für die Personen, deren Daten verarbeitet werden, darstellen können. Die Pflicht zur Meldung der Verfahren bei der Aufsichtsbehörde, die sogenannte Vorabkontrolle gem. § 4 d Abs. 5 BDSG, entfällt.

Ergibt sich bei der Risikoabschätzung der einzelnen Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten des Betroffenen, so muss eine Datenschutzfolgeabschätzung durchgeführt werden. Dies gilt insbesondere bei automatisierten Entscheidungen, massenhafter Verarbeitung von sensiblen Daten oder bei der Einführung neuer Technologien. Es erfolgt eine Bewertung des Risikos für die Verarbeitung der betroffenen, personenbezogenen Daten. Das Risiko eines Datenmissbrauchs dieser personenbezogenen Daten durch diese Verarbeitung ist durch geeignete technische und organisatorische Maßnahmen (TOM), die sich am neuesten Stand der Technik ausrichten, einzugrenzen. Die TOM sind nachvollziehbar zu dokumentieren.

Die Aufsichtsbehörden sind angehalten, Listen der Verarbeitungen zu erstellen, für die eine Datenschutzfolgenabschätzung notwendig ist. Bis diese Listen vorliegen, ist es ratsam, bei einem angenommenen hohen Risiko die Datenschutzfolgenabschätzung durchzuführen.

Können keine Maßnahmen zur Eindämmung des Risikos getroffen werden, muss die zuständige Aufsichtsbehörde konsultiert und ggfs. eine Genehmigung der Verarbeitung eingeholt werden.

## 4. Betrieblicher Datenschutzbeauftragter

Die Voraussetzungen, wann ein betrieblicher Datenschutzbeauftragter zu bestellen ist, wurden ebenfalls geändert.

Dies betrifft ab 25. Mai 2018 grundsätzlich alle Unternehmen, die besondere Arten von personenbezogenen Daten verarbeiten sowie alle Unternehmen mit mehr als 10 Mitarbeitern, die mit der Verarbeitung personenbezogener Daten befasst sind. Besondere Arten von personenbezogenen Daten sind beispielsweise Gesundheitsdaten, Informationen über Religion, politische Orientierung etc. Jedes Unternehmen, das im Gesundheitssektor Patientendaten verarbeitet, muss also einen Datenschutzbeauftragten bestellen. Ebenso jede politische oder kirchliche Einrichtung.

Dem Datenschutzbeauftragten kommt eine Überwachungsverpflichtung hinsichtlich der Einhaltung der vorstehend genannten Prozesse zu.

Es ist die Verantwortung des Datenschutzbeauftragten den Verantwortlichen zu unterrichten und zu beraten, die Einhaltung der EU-DSGVO, Einführung von internen Strategien, Zuweisung von Zuständigkeiten und Sensibilisierung sowie Schulung von Mitarbeitern zu überwachen und regelmäßig zu überprüfen

## 5. Auftragsdatenverarbeitung (innerhalb/außerhalb EU)

Sollten Daten im Auftrag verarbeitet werden sind einige Besonderheiten zu beachten.
Zunächst sind zukünftig sowohl der im Auftrag verarbeitende als **Verarbeiter und der Auftraggeber** als verantwortliche Stelle für die rechtmäßige und datenschutzkonforme Verarbeitung der Daten verantwortlich.

Das bedeutet: Als Auftraggeber muss man sich von der Zuverlässigkeit und Datenschutzkonformität des Beauftragten überzeugen und dies regelmäßig überprüfen.

Als Auftragnehmer muss man sicher sein, dass die Übermittlung und Beauftragung rechtmäßig ist, dass also insbesondere die Einwilligung der betroffenen Personen vorliegt.

Unabdingbar ist also ein Vertrag zur Auftragsdatenverarbeitung in dem die Rechte und Pflichten der Parteien festgehalten werden.

### Hinweise zur Vertragsgestaltung

Dieser Vertrag sollte so gestaltet sein, dass die Überwachung des Verarbeiters durch die verantwortliche Stelle möglich ist. Dies sollte auch ein Begehungsrecht und unangekündigte Kontrollen beinhalten. Außerdem sollte ein Weisungsrecht der verantwortlichen Stelle gegenüber dem Auftragsverarbeiter sichergestellt werden.

Ebenso sollten die Datenarten und die Verarbeitungsmethoden enthalten sein.

Diese Regelungen sind häufig bereits in einem Software License Agreement (SLA) des Auftragsverarbeiters enthalten. Falls nicht, sollte ein Annex zu diesem SLA geschlossen werden.

## Auftragsdatenverarbeitung außerhalb der EU

Sollte die Verarbeitung der Daten außerhalb der EU stattfinden, so finden die Vorschriften der EU-DSGVO dennoch Anwendung sofern die **Verantwortliche Stelle innerhalb der EU** ihren Sitz hat, oder Daten von sich **im EU-Gebiet aufhaltenden Personen** verarbeitet werden oder die Daten sich auf das **Verhalten von Personen innerhalb des EU-Gebietes** beziehen.

Für diesen Fall muss sichergestellt werden, dass der Sicherheitsstandard in dem Drittland dem Standard entspricht, den die EU-DSGVO voraussetzt. Dies kann entweder dadurch sichergestellt werden, dass das Drittland von der Aufsichtsbehörde oder über Abkommen als sicher eingestuft wurde oder durch den Abschluss von EU Model Clauses. Das ist ein Vertrag, der die Anforderungen an den Sicherheitsstandard definiert und dessen Einhaltung im Rahmen einer vertraglichen Verpflichtung sicherstellt.

## 6. Dokumentationspflichten

Die EU-DSGVO beinhaltet umfangreiche Dokumentationspflichten für jeden, der personenbezogene Daten erhebt, verarbeitet, speichert oder nutzt.

Es muss dokumentiert werden:

- Datenschutz-Managementsystem
- Datenschutz-Organisation
- Datenschutz-Policies
- Zuständigkeiten im Bereich des Datenschutzes
- Verarbeitungsvorgänge = Verfahrensverzeichnis
- Sensibilisierung & Schulung der Mitarbeiter
- Risikobewertungen
- Datenschutz-Folgenabschätzung
- Datenschutz-Verstöße/Vorfälle
- Löschkonzept
- Implementierte & durchgeführte Kontrollen – interne / externe Audits den Datenschutz betreffend

## 7. Haftungsfragen

Da die möglichen Bußgelder durch die EU-DSGVO stark verschärft wurden, stellt sich auch die Frage der Haftung mit größerer Dringlichkeit als bisher.

Hier kann man unterscheiden zwischen der **zivilrechtlichen Haftung** und der **strafrechtlichen Haftung.**

### a) Zivilrechtliche Haftung

- **Gegenüber der betroffenen Person**

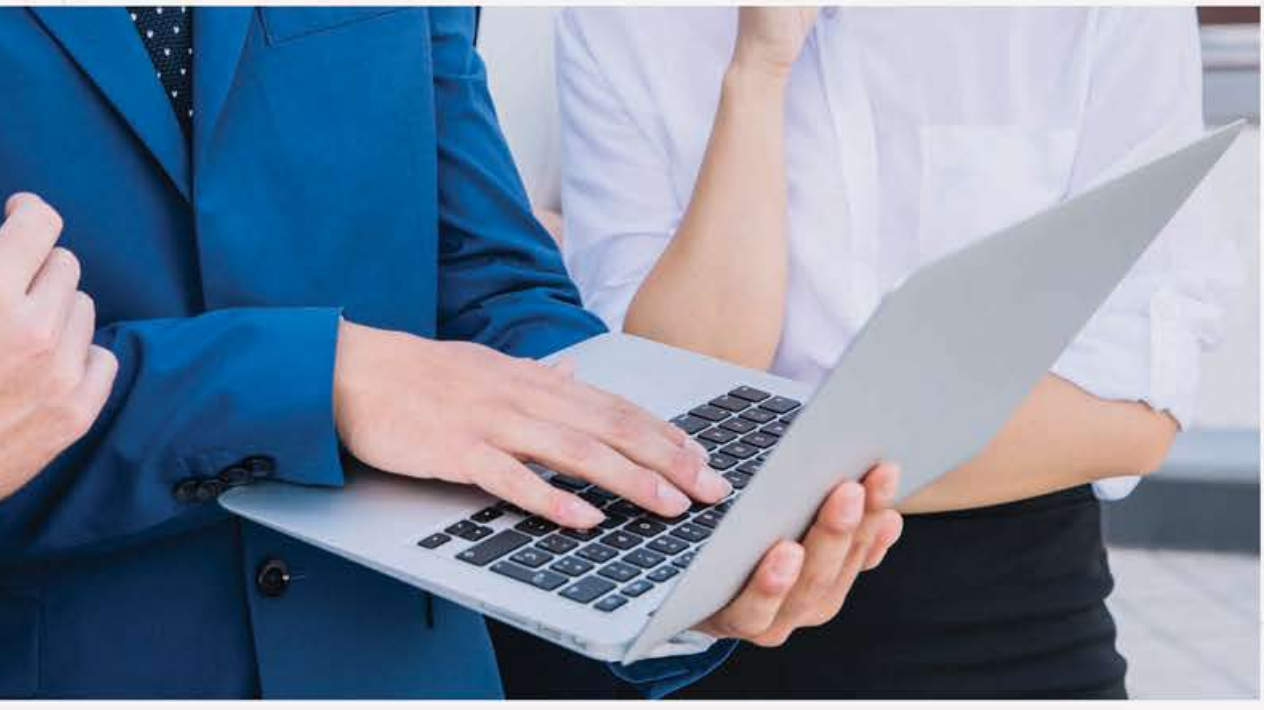
  Die Person, deren Daten verarbeitet werden, hat einen Anspruch auf Ersatz der materiellen und immateriellen Schäden, die ihr aufgrund einer Verletzung ihrer Rechte (fehlende Einwilligung, Verletzung von Schutzpflichten, Verlust, Veröffentlichung etc.) entstehen. Hierfür haften **sowohl die verantwortliche Stelle als auch der Verarbeiter** im Falle einer Auftragsverarbeitung. Die betroffene Person kann sich also an den liquideren wenden.
  In diesem Zusammenhang ist von besonderer Bedeutung, dass Verbandsklagen im Bereich des Datenschutzes zulässig sind. Es muss also nicht mehr die einzelne Person klagen, sondern Verfahren können auch von Verbraucherschutzverbänden o.ä. angestrengt werden. Ein erhöhtes Klageaufkommen ist also zu erwarten!

- **Aus dem Auftragsverarbeitungsverhältnis**

  Zivilrechtliche Ansprüche können sich auch aus dem Verhältnis zwischen Auftragsverarbeiter und verantwortlicher Stelle ergeben. Dies können beispielsweise Regressansprüche sein.

- **Regeressansprüche des Unternehmens gegen den Geschäftsführer, Vorstand, Datenschutzbeauftragten**

  Allerdings kann es auch sein, dass Unternehmen ihre Geschäftsführer, Vorstände und Datenschutzbeauftragten in Regress nehmen, wenn es zu Schäden gekommen ist.



### b) Strafrechtliche Haftung

Die strafrechtliche Haftung für Verstöße gegen Datenschutzvorschriften kann sich aus verschiedenen Gesetzen ergeben.

- **Strafgesetzbuch (StGB)**

  Das StGB sieht **Haftstrafen von bis zu drei Jahren** für Verstöße gegen Datengeheimnisse vor.

- **EU-DSGVO/ BDSG-neu**

  Die EU-DSGVO und das BDSG-neu sehen Bußgelder von **bis zu 20 Millionen Euro oder 4 % des globalen Konzernvorjahresumsatzes** vor, abhängig davon welcher Betrag höher ist.
  Dabei soll das Bußgeld wirksam, verhältnismäßig und **abschreckend** sein.

- **Telekommunikationsgesetz (TKG)**

  Das TKG sieht für Verstöße bis zu **500.000 Euro Bußgeld und bis zu zwei Jahre Haft** vor.

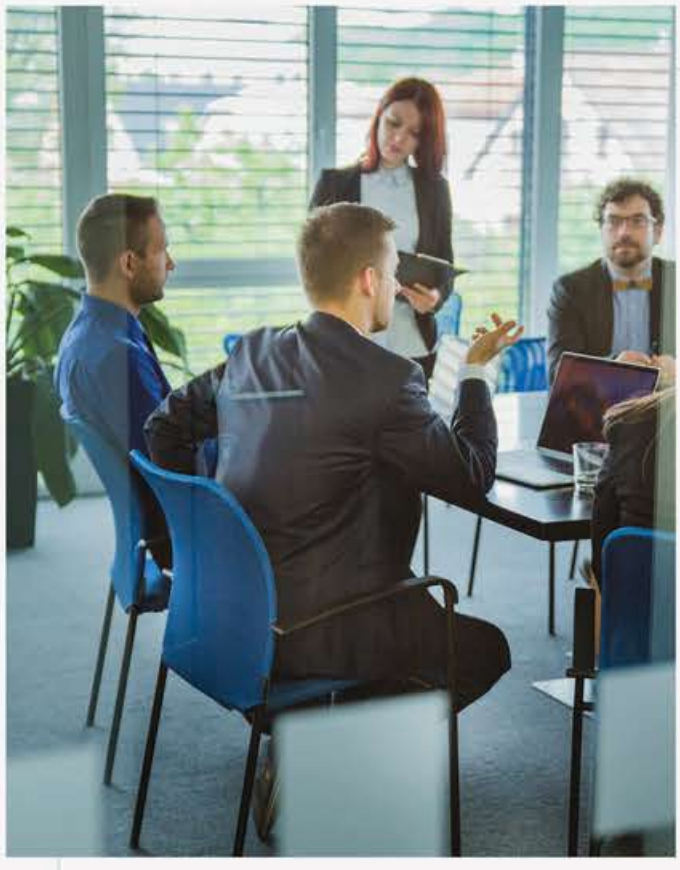
# C Welche Datenschutzprozesse müssen im Unternehmen bestehen?

## I. Dokumentation der Datenverarbeitungsprozesse im Unternehmen

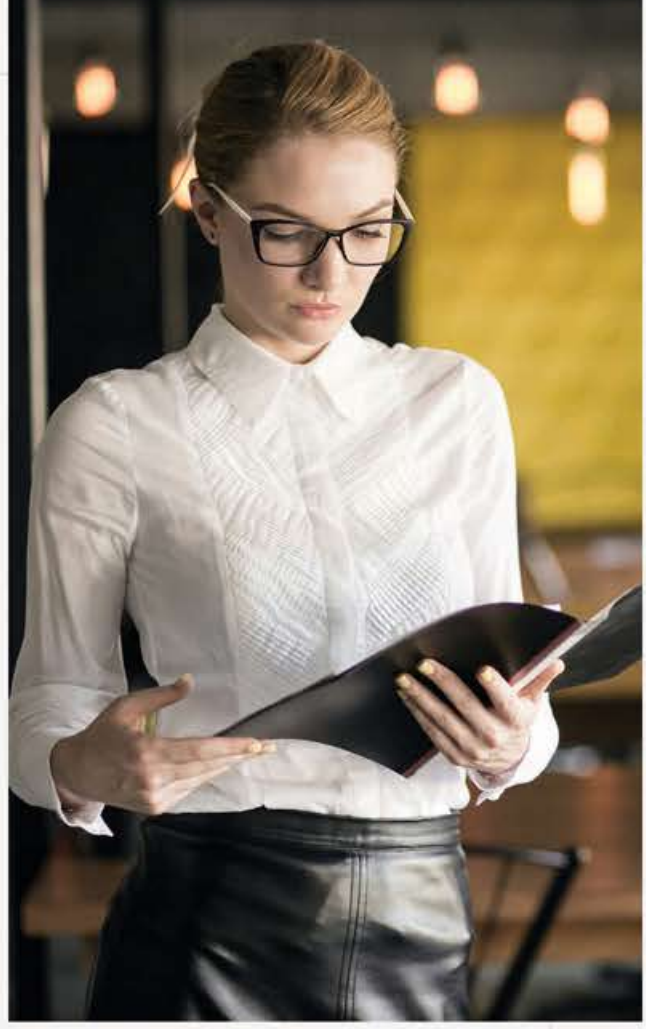
Zur Sicherstellung der Compliance im Hinblick auf die Regelungen der EU-DSGVO sind insbesondere die zukünftig bestehenden, erweiterten Dokumentationspflichten sicherzustellen.

Dokumentationspflichten bestehen zukünftig auch für Unternehmen, die Daten im Auftrag für Dritte verarbeiten (Auftragsverarbeiter).

Eine Auflistung der Dokumentationspflichten ist auf Seite 9 dieses Leitfadens.



Neben diesen prozessorientierten und systematischen Dokumentationspflichten ist es notwendig, die folgenden einzelnen Regelungen der EU-DSGVO sicherzustellen



## II. Erweiterung der Informationspflichten Art. 14 DSVGO – Dokumentation von Datenschutzerklärungen

Für alle Datenschutzerklärungen, die Mitarbeiter, Kunden oder sonstige Dritte gegenüber dem Unternehmen abgeben, gilt nach der EU-DSGVO eine Erweiterung der Informationspflichten. Dritte, deren Daten durch das Unternehmen verarbeitet werden, müssen zukünftig insbesondere hingewiesen werden auf

- die **Kontaktdaten** des Verarbeiters unter Angabe des Namens und der Anschrift des gesetzlichen Vertreters, Angabe der Kontaktdaten des Datenschutzbeauftragten,
- den **Zweck** der Verarbeitung und der bestehenden Rechtsgrundlage und im Fall der Zweckänderung das bestehende berechtigte Interesse des Verarbeiters zur Änderung des Zweckes gemäß Art. 6 Abs. 1 lit. (f) EU-DSGVO
- den **Empfänger** oder die Empfängerkategorien (sofern Daten übermittelt werden)
- eine **Übermittlung** in Drittländer außerhalb der EU mit Hinweis der bestehenden Sicherstellung des Datenschutzniveaus (z.B. EU – Standardverträge)
- die **Dauer** der Speicherung
- **Hinweise** zur automatisierten Entscheidungsfindung sowie auf die bestehenden Betroffenenrechte (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Datenübertragbarkeit, Beschwerde bei den Aufsichtsbehörden)

Im Hinblick auf die Compliance mit den Anforderungen der EU-DSGVO hat der Verarbeiter einen Prozess nachzuweisen, der die Einhaltung der vorstehenden Anforderungen dokumentiert.

## III. Prozess zur Abgabe und Widerruf von Einwilligungserklärungen

Im Hinblick auf Einwilligungserklärungen sind vor allem die verschärften formalen Vorgaben gemäß EU-DSGVO zu beachten. Zur Sicherstellung der Compliance muss ein Prozess für die Abgabe der Erklärung sowie den möglichen Widerruf der Einwilligung mit seinen systemtechnischen Auswirkungen implementiert und nachweisbar dokumentiert werden.

Einwilligungen gemäß Art. 6 Abs. 1 lit. (a) und Art. 7 der EU-DSGVO müssen zukünftig aufgrund einer eindeutigen Handlung erfolgen. Dies bedeutet, dass der Verarbeiter einen Nachweis über ein „**Opt-In**" erbringen muss. **Reine Untätigkeit ist keine Einwilligung**. Der Verarbeiter muss über sich selbst sowie Art und Zweck der Datenverarbeitung in einer klaren Sprache informieren. Die Information über den Zweck der Datenverarbeitung muss dabei konkret sein. Eine rein pauschale Angabe des Zwecks reicht nicht aus.

Im Hinblick auf die Freiwilligkeit wird eine **echte Wahlfreiheit** gefordert. Dem Betroffenen, der keine Einwilligung abgibt, dürfen dabei **keine Nachteile** entstehen. Der Verarbeiter darf zukünftig auch eine Einwilligung oder Vertragserfüllung nicht davon abhängig machen, dass der Betroffene in eine Datenverarbeitung einwilligt, die für die Erfüllung nicht notwendig ist. Aus einem Widerruf dürfen dem Betroffenen keinerlei Nachteile entstehen. Der **Widerruf** muss jederzeit mit Wirkung für die Zukunft möglich sein.

## IV. Dokumentation des Verfahrens zur Portabilität

Aufgrund der neuen Portabilitätsverpflichtung für Daten, müssen Verfahren bestehen, die sicherstellen, dass dem Betroffenen Daten, die er selbst zur Verfügung gestellt hat, wieder in einem gängigen Format zur Verfügung gestellt werden und ggf. auf Wunsch sogar direkt an Dritte übermittelt werden.

Um die Einhaltung der EU-DSGVO zu gewährleisten sind hierzu geeignete Prozesse mit Angabe der technischen und organisatorischen Maßnahmen zur Sicherstellung zu dokumentieren.

## V. Anpassung bestehender Betriebsvereinbarungen an EU-DSGVO

Die EU-DSGVO bietet gemäß Art. 88 EU-DSGVO iVm. § 26 BDSG-neu zukünftig im Einklang mit der bereits bestehenden Rechtsprechung des Bundesverfassungsgerichts die Möglichkeit, mit den Mitbestimmungsgremien basierend auf Betriebsvereinbarungen einen Erlaubnistatbestand zur rechtmäßigen Verarbeitung personenbezogener Daten zu vereinbaren.

Der Arbeitgeber als Verarbeiter muss dabei in diesen Betriebsvereinbarungen, die eine Verarbeitung von personenbezogenen Daten seiner Mitarbeiter und/oder Dritter regeln, geeignete und **konkrete Maßnahmen** beschreiben, die die folgenden Grundsätze der EU-DSGVO sicherstellen:

- Verarbeitung nach Treu und Glauben,
- Transparenz,
- klare Zweckdefinition und Zweckbindung,
- Datenminimierung (need to know),
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit (Datensicherheit) sowie Dokumentation der Verarbeitung zum Nachweis der Rechenschaftspflicht.

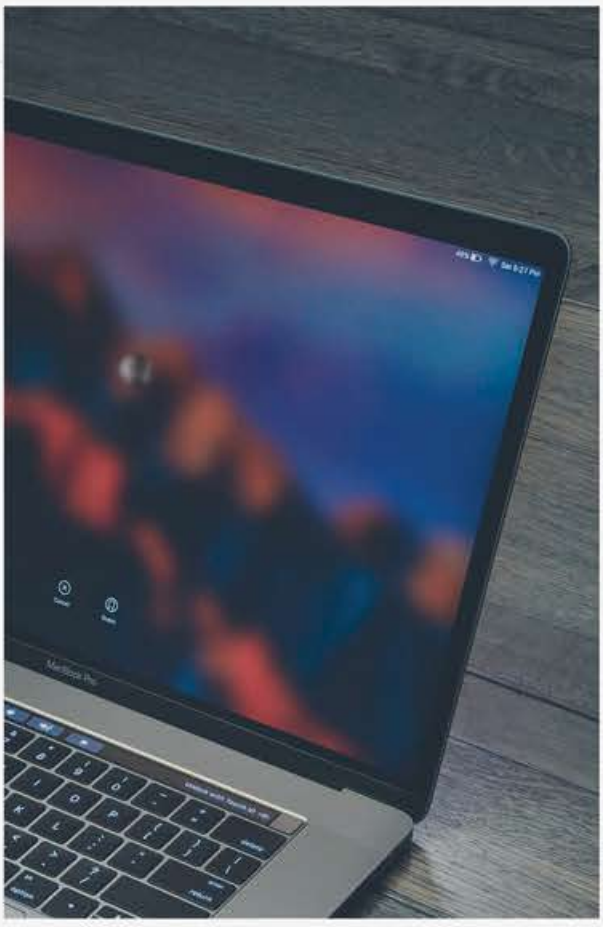
Insbesondere auf die TOM zur Sicherstellung der Datensicherheit ist hierbei einzugehen.

Bereits bestehende Betriebsvereinbarungen müssen unter dem vorstehend genannten Gesichtspunkt überarbeitet werden um nach dem 25. Mai 2018 weiterhin wirksam Bestand zu haben.

## VI. Nachweis der Vereinbarungen zur Auftragsverarbeitung

Inhaltlich regelt Art. 28 EU-DSGVO die in Deutschland bereits bekannten Punkte:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen,
- Umfang der Weisungsbefugnisse,
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit,
- Sicherstellung von technischen & organisatorischen Maßnahmen,
- Hinzuziehung von Subunternehmern,
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener,
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen,
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung, Kontrollrechte des für die Verarbeitung Verantwortlichen
- Duldungspflichten des Auftragsverarbeiters, Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt



Grundsätzlich bleibt der **für die Verarbeitung Verantwortliche** und nicht der Auftragsverarbeiter **erster Ansprechpartner** für Betroffene und für die Einhaltung der datenschutzrechtlichen Vorgaben.

Gegenüber dem Betroffenen **haften** zukünftig aber der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter gemeinsam.

Die Haftung des Auftragsverarbeiters ist dabei auf Verstöße gegen seine Pflichten als Auftragsverarbeiter beschränkt.

## VII. IT-Sicherheitsprüfung

Der Verantwortliche muss bei der Beauftragung neuer Dienstleister diese auf ihre IT-Sicherheit überprüfen. Insbesondere bei Cloud-basierten Systemen ergeben sich an dieser Stelle Besonderheiten.

Grundsätzlich werden bei einer IT-Sicherheitsprüfung die Technisch-Organisatorischen-Maßnahmen (TOMs) des Dienstleisters in Bezug auf das jeweilige Tool geprüft. Die TOMs des Dienstleisters für das Tool werden mit den eigenen Anforderungen an die IT-Sicherheit abgeglichen und bei Diskrepanzen die Risiken bewertet. Sodass die IT-Sicherheit des Tools festgestellt werden kann.

Bei Cloud-basierten Lösungen müssen zusätzlich zu den TOMs des jeweiligen Rechenzentrums auch die TOMs des Cloud-Anbieters überprüft werden.

Hilfreich bei einer IT-Sicherheitsprüfung können Nachweise des Dienstleisters zur IT-Sicherheit sein, z.B. eine ISO 27001 Zertifizierung.

## VIII. Schulungen zur EU-DSGVO und bestehenden eigenen Prozessen des internen

**Datenschutzkonzepts**

Die EU-DSGVO verpflichtet Unternehmen zu der Durchführung von zielgruppengerechten Schulungen. Bereits auf der Grundlage bisheriger EU-Datenschutzregelungen ist die Schulung von Mitarbeitern eine Anforderung. Zukünftig muss der Verantwortliche ein System in seinem Datenschutzkonzept dokumentieren, das systematische und zielgruppengerechte Schulungen nachweist. Systematische Schulungen können auch über die Dokumentation von Online-Schulungen geführt werden.

**System zur Durchführung von Risikobewertungen im Unternehmen mit Festlegung geeigneter technisch-organisatorischer Maßnahmen**

Gemäß der DSVGO werden im Hinblick auf die Compliance die Anforderung an die Festlegung geeigneter technisch-organisatorischer Maßnahmen geändert. Der Verantwortliche hat einen **risikobasierten Ansatz** bei der Bewertung der unternehmensinternen Risiken anzusetzen. Die tatsächliche Durchführung dieses risikobasierten Bewertungsansatzes ist als Risikoeinschätzung mit jeweils zum einzelnen Risiko geeigneten technisch-organisatorischen Maßnahmen gemäß Art. 32 EU-DSGVO zu dokumentieren.

**Einführung der Dokumentation der Risikofolgeabschätzung**

Im Hinblick auf datenschutzrechtliche Compliance muss im Datenschutzkonzept ein **Verfahren** festlegt werden, dass jeweils die Zuständigkeiten bei der Durchführung der Datenschutzfolgeabschätzung regelt.

## IX. Datenpannen – erweiterte Obliegenheiten

Im Fall einer Datenpanne besteht gemäß EU-DSGVO die Verpflichtung, den Vorfall, der ein Risiko für die Rechte und Pflichten der Betroffenen darstellt, **innerhalb von 72 Stunden** zu der Aufsichtsbehörde zu melden.

Zusätzlich muss auch der Betroffene informiert werden, wenn die Datenpanne voraussichtlich zu einem hohen Risiko für seine personenbezogenen Daten führt.

Für beide Informationsverpflichtungen gilt, dass hierzu **interne Richtlinien** bestehen müssen, die diesen Prozess nachweisbar festhalten und die Mindestanforderungen an den Inhalt einer solchen Meldung gemäß Art. 33 Absatz 3 EU-DSGVO beachten.

Teil des Datenschutzkonzepts zur Sicherstellung der Compliance mit der EU-DSGVO ist die Darstellung des bestehenden, internen Prozesses zur Bearbeitung von Datenpannen.

Hierbei sind Zuständigkeiten, Ansprechpartner, Informationspflichten festzuhalten.

Bereichsspezifisch sollte die Definition zur **Zuständigkeit** der Abhilfe im Fall des Datenverstoßes, Sicherung der Daten, Korrektur von Daten und Meldung von Verstößen an die Aufsichtsbehörde und den Betroffenen innerhalb des Datenschutzkonzeptes definiert werden.

Dabei definiert die EU-DSGVO eine Ausweitung der Meldepflicht bei Datenpannen an eine Aufsichtsbehörde auf **jeden Vorfall**, der ein „Risiko" für die Rechte und Pflichten der Betroffenen darstellt binnen 72 Stunden. Zusätzlich muss auch der Betroffene unverzüglich über eine Datenpanne informiert werden, wenn sie „voraussichtlich" zu einem „hohen Risiko" führt.

Die zuständige Aufsichtsbehörde für ein Unternehmen richtet sich dabei europaweit nach dem Hauptsitz bzw. der Niederlassung, die generell über die Datenverarbeitung entscheidet.

## D Backdoor-freie Software

Um die Compliance im Hinblick auf die im Unternehmen verwendete Softwareapplikationen sicherzustellen, sollte zusätzlich als Vorgabe die Verwendung von ausschließlich Backdoor-freier Software gelten. Bund, Länder und Kommunen sind verpflichtet ausschließlich auf IT-Dienstleister zurückzugreifen, die nachweislich keine Backdoors in ihrem Betriebssystem haben.

Es sollte eine Überprüfung der unternehmensinternen Security-Anbieter im Hinblick auf die Backdoors (unauthorised Code) im Hinblick auf die verwendeten Betriebssysteme erfolgen.

Bei Softwareprodukten ist eine freie Einsicht in deren Quellcode ein wichtiger Aspekt der Computersicherheit. Hierdurch soll das Risiko eingeschränkt werden, dass die Software heimliche Funktionen enthalten kann, wie die einer Backdoor.

Über eine Backdoor, kann sich ein Angreifer unbemerkt Zugang zum Betriebssystem verschaffen. Die Zugriffssicherungen des Systems werden umgangen, die Daten des Unternehmens und damit auch die der EU-DSGVO unterworfenen personenbezogenen Daten können unberechtigt eingesehen werden.
**Ein Datenverstoß liegt vor.**

Daher sollten Unternehmen und Organisationen nur Backdoor-freie Anbieter in die engere Auswahl für ihre IT-Sicherheitslösungen nehmen, die eine Minimierung dieses Risikos für einen Datenverstoß ermöglichen und dem behördlichen Anforderungsprofil entsprechen.

# E EU-DSGVO – möglicher Fahrplan eines EU-DSGVO Projekts:

Die einzelnen Prozessschritte zur Umsetzung der Inhalte der EU-DSGVO werden sich am jeweils vorhandenen Datenschutzprozess eines Unternehmens orientieren. Die nachstehenden Schritte können als mögliche Anhaltspunkte für einen Umsetzungsprozess dienen.

a. Definition eines Projektteams mit Verantwortlichkeiten; insbesondere Einbeziehung des Datenschutzbeauftragten und IT Security Verantwortlichen

b. Ressourcenplanung und Budgetplanung

c. Analyse vorhandener Datenschutzprozesse Soll – Ist Vergleich: hieraus ermittelt sich der jeweilige Handlungsbedarf

d. Analyse der bestehenden, datenverarbeitenden „Applikationen" – Bestandsaufnahme - Data Mapping

e. Prüfung besehender Datenschutzprozesse auf Bestehen eines Erlaubnistatbestandes im Sinne der DSVGO

f. Durchführung der Datenschutz-Folgeabschätzung (DPIA) für besondere Risiken und Dokumentation der DPIA

g. Datenschutztrainings für Mitarbeiter

h. Kommunikation mit den Beteiligungsgremien / Betriebsrat

i. Anpassung einzelner Prozesse und Schließen von Lücken mit Dokumentation

- Prüfung und ggf. Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten
- Anpassung der Datenschutzorganisation; ggf. Bestellung eines Datenschutzbeauftragten
- Prüfung der Prozesse im Fall von Datenpannen und Implementierung von Prozessen bezüglich Meldepflichten
- Anpassung der Dienstleistungsbeziehungen, Schwerpunkt ADV Verträge und EU – Model Clauses mit Dienstleistern in Drittländern (nicht EU/EWR)
- Anpassung der IT-Sicherheit: Prüfung des Unternehmens und Sicherstellen der Cyber und IT – Sicherheit durch z.B. IT - Prozessbeschreibungen, aktualisierte TOMs, gültige Zertifikate
- ggf. Anpassung von Betriebsvereinbarungen

**Die Autoren**

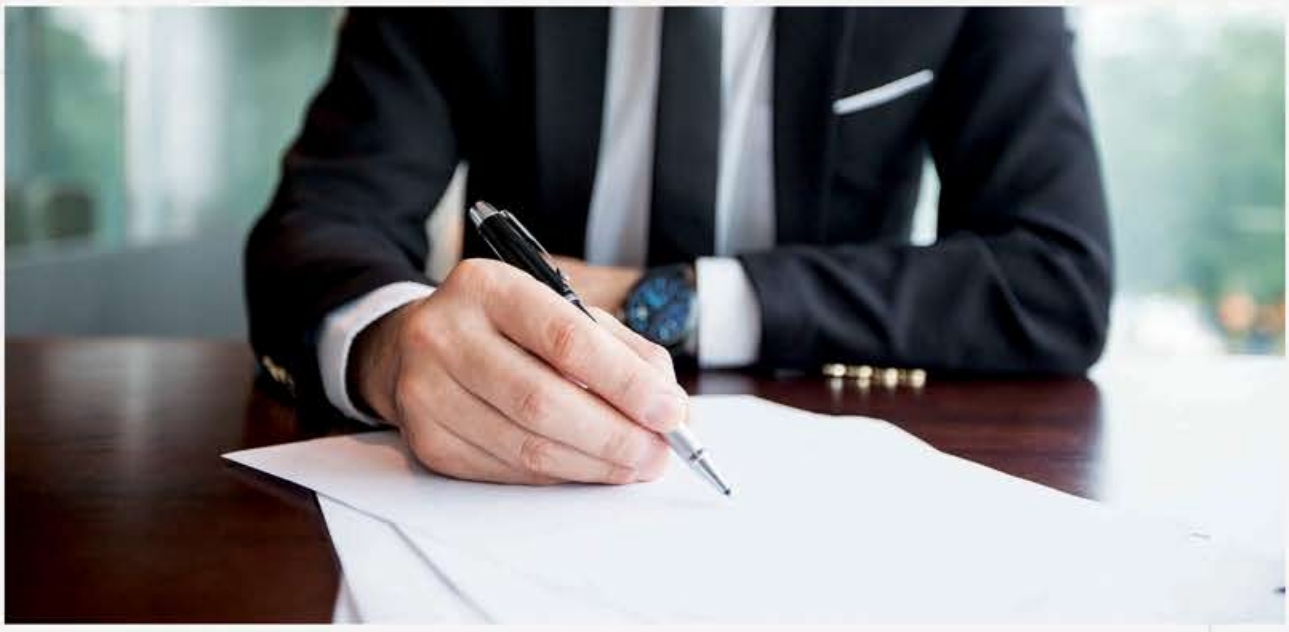
RA Robert Niedermeier ist seit 25 Jahren als externer Datenschutzbeauftragter in ganz Europa tätig (www.cyberlegal.eu). Im Ehrenamt arbeitet er als Executive Secretary beim European Institute for Computer Anti-Virus Research (www.eicar.org) an der Schnittstelle von Recht und IT.

RAin Gummermann ist als externe Datenschutzbeauftragte zertifiziert, verfügt über mehr als 25 Jahre Erfahrung im Bereich internationale Verträge, IT Recht und leitet Projekte zur Einführung der EU-DSGVO. Als Anwältin berät Sie Mandanten mit internationaler Konzernstruktur in den Bereichen Datenschutz, Datensicherheit und IT-Recht mit Schwerpunkt vertraglicher Sicherstellung der gemäß EU Datenschutz geforderten Datenschutz Garantien (EU Model Clauses / BCR). (www.cyberlegal.de).

RAin Dorothea Teichmann ist seit April 2017 im Bereich Prüfung und Sicherstellung von Verträgen zur Einhaltung des EU Datenschutzes, Datensicherheit und IT-Recht für die Rechtsanwaltskanzlei Niedermeier & Faulhaber Partnerschaft mbH Cyberlegal zuständig.

**Haftungshinweis zur Nutzung des Leitfadens:**

**Dieses Dokument stellt per se nur einen allgemeinen Leitfaden dar, der Hinweise für eine Vielzahl von Fallkonstellationen gibt. Er ist nicht als verbindliche Rechtsauskunft zu betrachten, da letztendlich immer eine Einzelfallprüfung anhand des spezifischen Unternehmensgepräges vorzunehmen ist. Der Leitfaden kann somit eine individuelle rechtliche Beratung nicht ersetzen.**



# F Checkliste

## Allgemein

- [ ] Implementierung des Informationssicherheitskonzepts gemäß EU-DSGVO, BDSG-neu, KonTraG, BASEL III, IT-Sicherheitsgesetz (betrifft KRITIS) und weitere branchenspezifische Spezialgesetze
- [ ] Definition geeigneter Administratoren und deren Zuständigkeiten
- [ ] Prüfung der bestehenden Rollenkonzepte einzelner im Unternehmen verwendeter Softwareanwendungen
- [ ] Datenschutzfolgenabschätzung (Vorprüfung von Verarbeitungsvorgängen)
- [ ] Implementierung geeigneter technischer und organisatorischer Maßnahmen (TOM), die sich am neuesten Stand der Technik ausrichten
- [ ] Ernennung/Bestellung eines betrieblichen Datenschutzbeauftragten
- [ ] Portabilität der Daten ist sichergestellt und dokumentiert
- [ ] Es wird ein risikobasierter Ansatz bei der Bewertung der unternehmensinternen Risiken verwendet
- [ ] Systematische Schulung der Mitarbeiter
- [ ] Nutzung Backdoor-freier Lösungen

### Pflicht für Auftraggeber:

[ ] Prüfung der Zuverlässigkeit und Datenschutzkonformität des Beauftragten

### Pflicht für Auftragnehmer:

[ ] Prüfung der Rechtmäßigkeit der Übermittlung und Beauftragung (Einwilligung der betroffenen Personen)

### Vertragsgestaltung zur Auftragsdatenverarbeitung

[ ] Möglichkeit zur Überwachung des Verarbeiters durch die verantwortliche Stelle

[ ] Sicherstellung eines Weisungsrechts der verantwortlichen Stelle gegenüber dem Auftragsverarbeiter

[ ] Aufnahme der Datenarten und die Verarbeitungsmethoden

[ ] Annex zu bestehenden SLA falls notwendig

### Geltung der EU-DSGVO bei Auftragsdatenverarbeitung außerhalb der EU

[ ] Verantwortliche Stelle hat Sitz innerhalb der EU

[ ] Verarbeitung von Daten von sich im EU-Gebiet aufhaltenden Personen

[ ] Verarbeitung von Daten, die sich auf das Verhalten von Personen innerhalb des EU-Gebietes beziehen

### Dokumentationspflichten

[ ] Datenschutz-Managementsystem

[ ] Datenschutz-Organisation

[ ] Datenschutz-Policies

[ ] Zuständigkeiten im Bereich des Datenschutzes

[ ] Verarbeitungsvorgänge = Verfahrensverzeichnis

[ ] Sensibilisierung & Schulung der Mitarbeiter

[ ] Risikobewertungen

[ ] Datenschutz-Folgenabschätzung

[ ] Datenschutz-Verstöße/Vorfälle

[ ] Löschkonzept

[ ] Implementierte & durchgeführte Kontrollen – interne / externe Audits den Datenschutz betreffend

### Informationspflichten / Dokumentation von Datenschutzerklärungen

- [ ] Kontaktdaten des Verarbeiters unter Angabe des Namens und der Anschrift des gesetzlichen Vertreters, Angabe der Kontaktdaten des Datenschutzbeauftragten,
- [ ] Zweck der Verarbeitung und der bestehenden Rechtsgrundlage
- [ ] Empfänger oder die Empfängerkategorien (sofern Daten übermittelt werden)
- [ ] Übermittlung in Drittländer außerhalb der EU mit Hinweis der bestehenden Sicherstellung des Datenschutzniveaus
- [ ] Dauer der Speicherung
- [ ] Hinweise zur automatisierten Entscheidungsfindung sowie auf die bestehenden Betroffenenrechte
- [ ] Nachweis eines Prozesses, der die Einhaltung der vorstehenden Anforderungen dokumentiert.

### Abgabe und Widerruf von Einwilligungserklärungen

- [ ] Prozess für die Abgabe der Erklärung sowie den möglichen Widerruf der Einwilligung mit seinen systemtechnischen Auswirkungen ist implementiert und nachweisbar dokumentiert.
- [ ] Einwilligung nur durch eindeutige Handlung (Opt-In)
- [ ] Information zu Art und konkretem Zweck der Datenverarbeitung in klarer Sprache

- [ ] Keine Nachteile durch Nichteinwilligung oder Widerruf
- [ ] Widerruf ist jederzeit mit Wirkung für die Zukunft möglich

### Anpassung bestehender Betriebsvereinbarungen

- [ ] Verarbeitung nach Treu und Glauben
- [ ] Transparenz
- [ ] klare Zweckdefinition und Zweckbindung
- [ ] Datenminimierung (need to know)
- [ ] Richtigkeit
- [ ] Speicherbegrenzung
- [ ] Integrität und Vertraulichkeit (Datensicherheit)
- [ ] Dokumentation der Verarbeitung zum Nachweis der Rechenschaftspflicht

## Nachweis der Vereinbarungen zur Auftragsverarbeitung

[ ] Gegenstand und Dauer der Verarbeitung

[ ] Art und Zweck der Verarbeitung

[ ] Art der personenbezogenen Daten & Kategorien von betroffenen Personen

[ ] Umfang der Weisungsbefugnisse

[ ] Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit

[ ] Sicherstellung von technischen & organisatorischen Maßnahmen

[ ] Hinzuziehung von Subunternehmern

[ ] Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener

[ ] Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen

[ ] Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung, Kontrollrechte des für die Verarbeitung Verantwortlichen

[ ] Duldungspflichten des Auftragsverarbeiters, Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

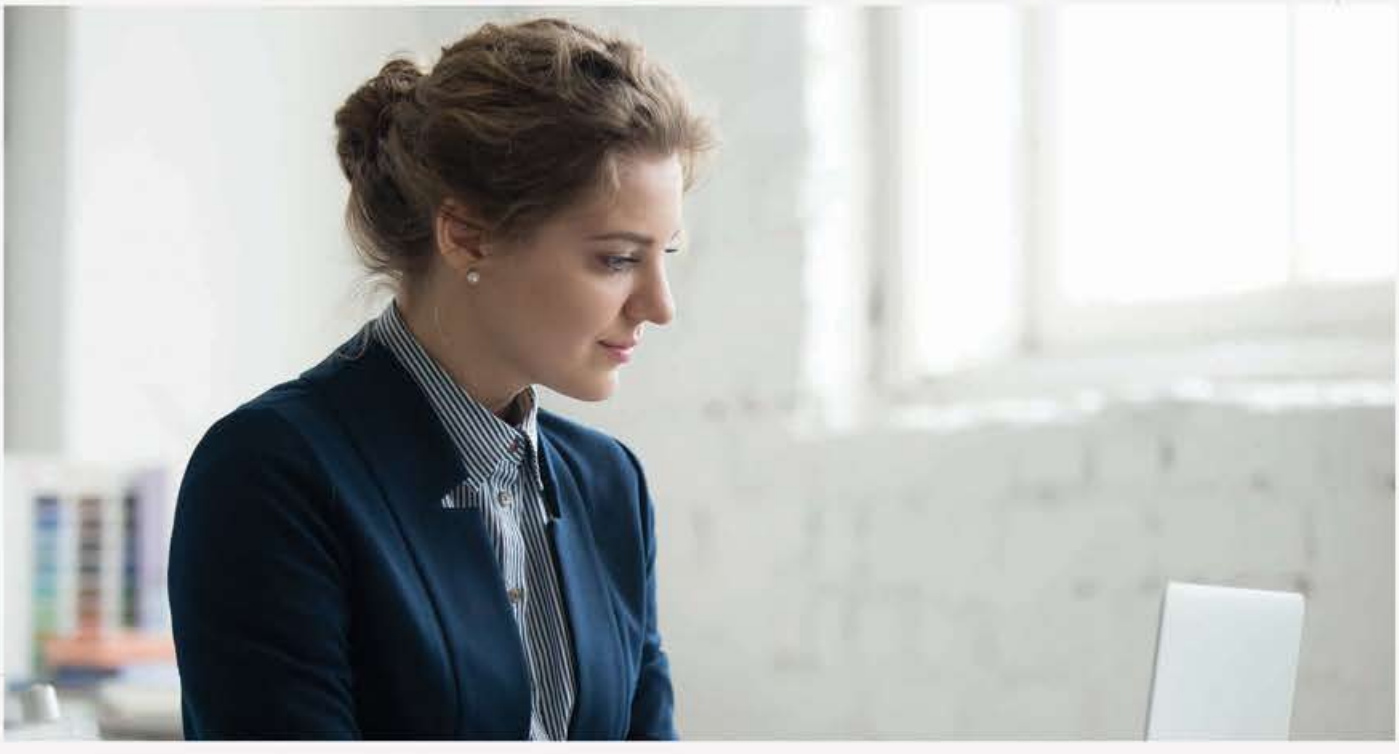
## Im Falle einer Datenpanne

[ ] Innerhalb von 72 Stunden Meldung an die Aufsichtsbehörde

[ ] Bei hohem Risiko für personenbezogenen Daten: Information der Betroffenen

[ ] Es bestehen interne Richtlinien, die diesen Prozess nachweisbar festhalten und die Mindestanforderungen an den Inhalt einer solchen Meldung beachten

[ ] Definierte Zuständigkeiten, Ansprechpartner, Informationspflichten sind festgehalten



## Rohde & Schwarz Cybersecurity:
## Lösungsportfolio für die organisatorischen und technischen Herausforderungen der DSGVO

Unser konzeptioneller Ansatz zur termingerechten Implementierung der DSGVO und dauerhaften Aufrechterhaltung der Datenschutz-Compliance in Kombination mit der Einführung eines Informationssicherheitsmanagements (ISMS) bietet mit einsatzfähigen Lösungen besondere Vorteile.

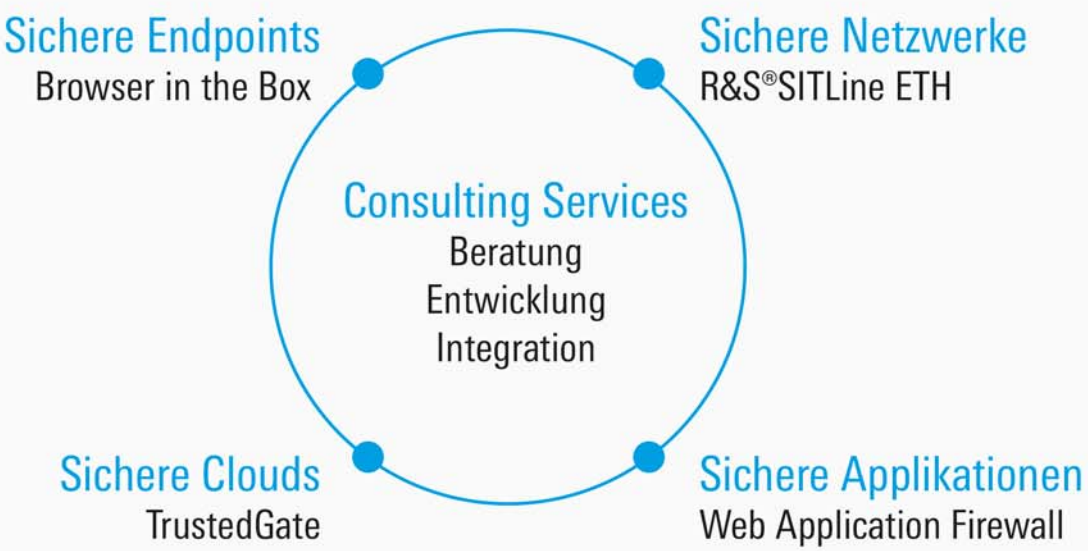
Dank eines breiten Portfolios von **IT-Sicherheitslösungen** aus einer Hand und umfassender Expertise in der **IT-Security-Beratung**, ist Rohde & Schwarz Cybersecurity Ihr verlässlicher Partner für die organisatorische und technische Implementierung der DSGVO in Ihrem Unternehmen. Unsere Sicherheitslösungen entsprechen den höchsten europäischen Compliance-Standards und dem aktuellen Stand der Technik. Zudem verfolgen wir eine strikte „No-Backdoor-Policy“. All unsere Produkte sind somit frei von Hintertüren, die potenziell als Angriffsvehikel genutzt werden können.

Rohde & Schwarz Cybersecurity bietet Hochleistungsverschlüsseler, die Verbindungen zwischen Rechenzentren und Standorten (WAN) vor Cyberangriffen und Überlastung der Netzwerke schützen. **R&S®SITLine ETH**, unsere Gerätefamilie für Ethernet-Verschlüsselung, erlaubt die Steigerung des Verschlüsselungsdurchsatzes auf bis zu 40 Gbit/s pro Gerät. Der Krypto-Durchsatz kann dabei ohne Gerätetausch per Software-Upgrade an die Unternehmensanforderungen angepasst werden.

**Browser in the Box** bietet proaktiven Schutz gegen Cyberangriffe. Dank der sicheren Trennung des Browsers von den restlichen Bereichen des PCs bleiben personenbezogene Daten jederzeit geschützt. Durch das Management-Tool konfigurieren Sie Sicherheitsrichtlinien und Compliance-Vorgaben.

**TrustedGate** ermöglicht sicheres und datenschutzkonformes Arbeiten in Cloud-Umgebungen und Collaboration-Tools. Mittels Verschlüsselung und Fragmentierung bleiben sensible Unternehmensdaten und Dokumente in einer festgelegten Region, gleichzeitig wird eine Zusammenarbeit in der Cloud global ermöglicht.

Mit unseren Lösungen für sichere webbasierte Applikationen, wie der **Web Application Firewall**, bieten wir ein ganzheitliches Produktportfolio für die datenschutzkonforme Handhabung sensibler Kundendaten, wie beispielsweise von Finanzdienstleistern, E-Commerce-Shops und Versicherungen.



# Praxisleitfaden zur Datenschutz-Grundverordnung (EU-DSGVO) aus Compliance-Sicht

cyberlegal

ROHDE&SCHWARZ
Cybersecurity

eicar
EXPERT GROUP FOR IT-SECURITY