



# QTA – Jahrestagung



# Neues Datenschutzrecht - ab dem 25.05.2018 -



# EU-Datenschutzgrundverordnung (DSGVO)

Seite 3  
19.05.2018

**DSGVO gilt ab dem 25.05.2018  
unmittelbar**

**Ziel Harmonisierung des  
Datenschutzes in der EU**

**Bundestag hat ergänzend neues BDSG  
erlassen**



# Erwägungsgründe

„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.“



# EU-Datenschutzgrundverordnung (DSGVO)

Seite 5

19.05.2018

**Verbesserung des Datenschutzes**

**Stärkung der Betroffenenrechte**

**Recht auf Auskunft, Berichtigung, Löschung  
(Vergessenwerden), Einschränkung der Verarbeitung,  
Widerspruch und Recht zur Datenübertragung**



# Verantwortliche Stelle

**Verantwortliche Stelle ist jedes Unternehmen, welches personenbezogene Daten verarbeitet, also auch die Reisebüros!**



# Neues Datenschutzrecht ist strenger!

**Bei Verstößen droht Geldbuße von bis zu 4 % des Umsatzes oder bis zu 20 Mio. €, Art. 83 DSGVO.**

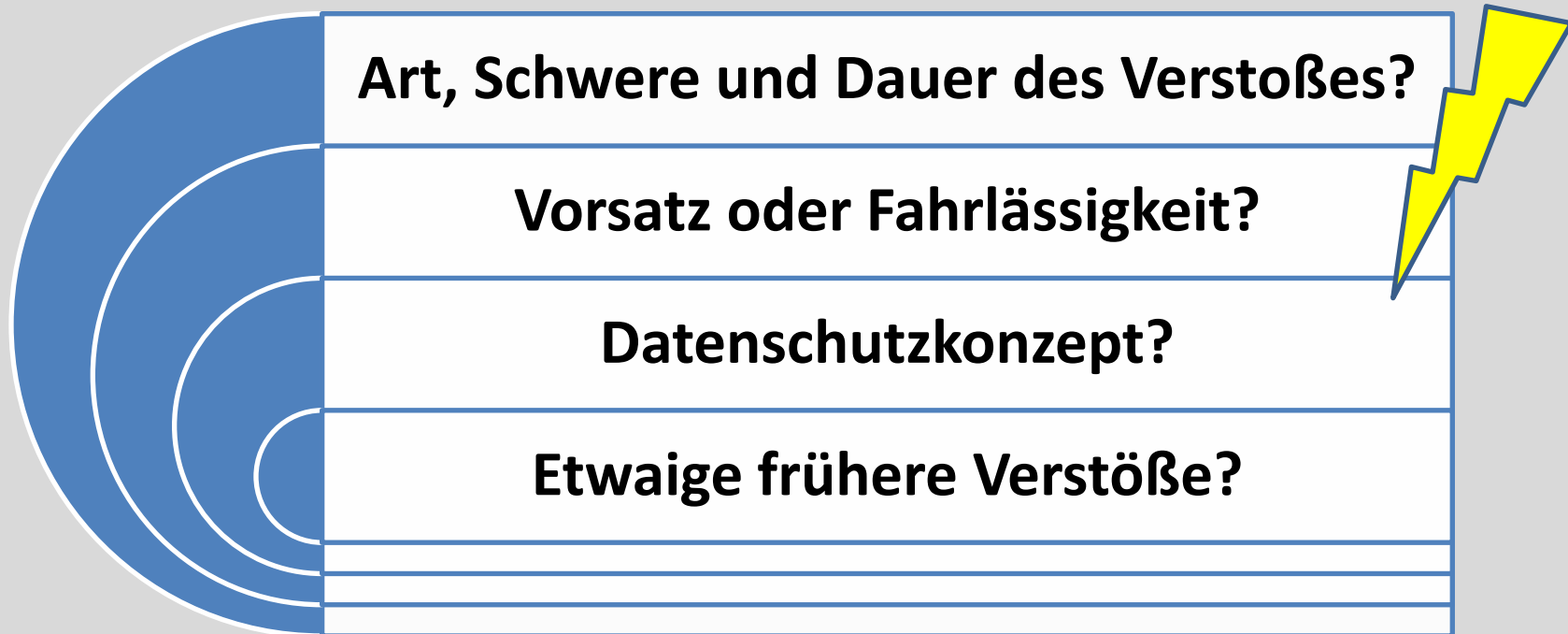
**Der Betroffene hat Anspruch auf Ersatz des materiellen und immateriellen Schadens, Art. 82 Abs. 2 DSGVO.**

**Verbraucherschutzverbände haben eigenes Klagerecht.**

**Nach Art. 24 Abs. 1 DSGVO gilt Beweislastumkehr.**



# Bußgeldkriterien nach der DSGVO







# Neues Datenschutzrecht





# Prüfpflicht: Wann ist die Verarbeitung persönlicher Daten zulässig?

Verarbeitung zur Vertragserfüllung (z. B. Buchungen)

Verarbeitung aufgrund gesetzlicher Verpflichtung  
(z. B. Meldung an Sozialversicherungsträger)

Verarbeitung aufgrund einer Einwilligung des  
Betroffenen (z. B. bei Direkt-Mailing)

Verarbeitung zur Wahrnehmung berechtigter  
Interessen (z. B. Briefwerbung)



# Voraussetzungen der Einwilligung

**Information über Umfang  
und Zweck der  
Verarbeitung**

**Einfache und klare Sprache  
sowie Abgrenzung von  
anderen Sachverhalten**

**Kopplungsverbot**

**Hinweis auf kostenfreies  
Widerrufsrecht**



# Wann ist eine Einwilligung erforderlich?

Seite 12  
19.05.2018

## Fall:

RB möchte eine Direktmarketingaktion bei Bestandskunden und neuen potentiellen Kunden per E-Mail, SMS, Fax, Telefonanruf und/oder Briefwerbung durchführen.

Ist dafür eine Einwilligung erforderlich?



# Erforderlichkeit einer Einwilligung

## Eine Einwilligung ist erforderlich:

- Bei Direktmarketing gegenüber Neukunden per E-Mail, SMS, Fax und Telefonanruf.
- Bei Bestandskunden im Wege E-Mail, SMS, Fax und Telefonanruf.
- Hingegen ist die reine Briefwerbung auf Basis von sog. Listendaten ohne Einwilligung zulässig!



## Was ist mit meinen alten Einwilligungserklärungen?



- Alte Erklärungen können weiter verwendet, soweit sie die Voraussetzungen von Art. 7 DSGVO erfüllen.
- Achtung: Von den alten Einwilligungserklärungen muss das RB regelmäßig Gebrauch gemacht haben.
- Soweit die Einwilligungserklärungen nicht DSGVO-konform sind, muss eine neue Einwilligungserklärung eingeholt werden.



# Form der Einwilligung

## Form der Einwilligung:

Das RB muss nachweisen können, dass eine wirksame Einwilligung vorliegt, vgl. Art. 7 Abs. 1 DSGVO.

Daher ist die Schriftform zu empfehlen.

Beim Newsletter-Versand per E-Mail ist das Double OptIn-Verfahren zu beachten.

Die Einwilligungserklärungen müssen archiviert werden.



## Double OptIn-Verfahren:

**Abonnement erhält  
nach Anmeldung  
werbefrei  
Bestätigungs-Mail.**

**Erst nach Zugang  
der Bestätigungs-  
Mail erhält der  
Abonnement den  
Newsletter.**

**Andere Verfahren, z.  
B. OptIn-Verfahren  
oder OptOut-  
Verfahren sind nicht  
abmahnsicher!**





# Fehler beim Direktmarketing

## Typische Fehler beim Direktmarketing:

1. Kein Double OptIn-Verfahren
2. Werbung in der Bestätigungs-Mail
3. Kein Hinweis auf kostenfreies Widerrufsrecht
4. Weitere Werbe-Mail trotz Widerruf
5. Direktmarketing auf Basis ungültiger Einwilligungen
6. Kein Impressum
7. Telefonanrufe bei Bestandskunden ohne Einwilligung
8. Gewinnspiel mit gekoppelter Einwilligung



## Hinweis:

Soweit Widerruf erfolgt, sind die Daten für  
Werbemaßnahmen zu löschen, Art. 17 Abs. 1 DSGVO.



# Dokumentationspflichten

## **Art. 24 Abs. 1:**

**Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.**



# Dokumentationspflichten

**Das RB muss nachweisen können, dass die Datenverarbeitung rechtskonform erfolgt.**



**Dies macht neben der Vornahme technischer-organisatorischer Maßnahmen auch deren Dokumentation erforderlich!**



# Dokumentationspflichten - Überblick

Seite 21  
19.05.2018

- **Verarbeitungsverzeichnis (VVZ)**
- **Datenschutzerklärung**
- **Auftragsverarbeitung (ADV)**
- **Verpflichtung auf das Datengeheimnis**
- **Festlegung der Verantwortlichkeiten**
- **Benennung des  
Datenschutzbeauftragten (soweit  
erforderlich)**



# Verarbeitungsverzeichnis

***„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche ein Verzeichnis der Verarbeitungstätigkeiten führen. Jeder Verantwortliche sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“***



# Verzeichnis von Verarbeitungstätigkeiten

Seite 23  
19.05.2018

Namen und  
Kontaktdaten  
des Verant-  
wortlichen

Zwecke der  
Verarbeitung

Kategorien von  
betroffenen  
Personen und  
Daten

Kategorien von  
Empfängern,  
an die die  
Daten  
weitergegeben  
werden (auch  
in Drittländern)

Löschfristen



# Informationspflichten bei Datenerhebung

**Das Reisebüro XY, Inhaberin Frau Musterfrau, Musterstraße 1, 12345 Musterstadt, erhebt Ihre Daten zum Zweck der Vertragsdurchführung, zur Erfüllung ihrer vertraglichen und vorvertraglichen Pflichten.**

**Die Datenerhebung und Datenverarbeitung ist für die Durchführung des Vertrags erforderlich und beruht auf Artikel 6 Abs. 1 b) DSGVO. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind, es sei denn, dass wir nach Artikel 6 Abs. 1 S. 1 lit. c DSGVO aufgrund von steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten zu einer längeren Speicherung verpflichtet sind oder Sie in eine darüber hinausgehende Speicherung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO eingewilligt haben. Zudem sind Sie berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern... Sie können unseren Datenschutzbeauftragten unter [datenschutz@reisebuero.de](mailto:datenschutz@reisebuero.de) oder unter Datenschutzbeauftragter c/o Reisebüro XY, Musterstraße 1, 12345 Musterstadt, erreichen.**

**Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.**





# Auftragsverarbeitung

## Auftragsverarbeitung:

- Weitergabe von personenbezogenen Daten an Dritte zur auftragsgemäßen Verarbeitung
- Zusammenarbeit nur mit zuverlässigen Partnern, vgl. Art. 28 Abs. 1 DSGVO



# Anwendungsbereich

## Anwendungsbereich:

- AV müssen abgeschlossen werden mit IT-Dienstleistern, Buchhaltungsfirmen, Marketingdienstleistern

## Keine Anwendungsfälle sind:

- Einschaltung von Putzfirmen und Hausmeisterdiensten  
(Geheimhaltungsvereinbarung erforderlich!)
- Datenweitergabe an Reiseveranstalter / Leistungsträger für die Buchung
- Einschaltung von Rechtsanwälten und Steuerberater



## Inhalt der AV

- Vertrag nach Art. 28 Abs. 9 DSGVO in schriftlicher oder elektronischer Form abzuschließen.
- Pflichtinhalte der AV ergibt sich aus Art. 28 Abs. 3 a - h DSGVO.
- Dienstleister sollten Nachweise für die Einhaltung der TOM'S erbringen.
- Im Verletzungsfall besteht eine gemeinsame Verantwortung.



# Informationspflichten

## Fall:

**U hat eigene Webseite. Eine Datenschutzerklärung fehlt.**

**Verbraucherschutzverband V mahnt den U ab.**

**Zu Recht?**



# Informationspflichten

**Jeder Webseitenbetreiber benötigt eine vollständige Datenschutzerklärung.**

**Webseitenbetreiber die keine oder nur eine unvollständige Datenschutzerklärung haben, verstoßen gegen das Wettbewerbsrecht (vgl. LG Hamburg v. Urt. 07.01.2016).**

**Seit Oktober 2016 gilt zudem das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von Verbraucherschützenden Vorschriften des Datenschutzrechts.**



# Inhalt der Datenschutzerklärung

Verarbeitung persönlicher Daten

Cookies, Newsletter und Social Media

Speicherdauer

Betroffenenrechte

Kontaktdaten des Datenschutzbeauftragten

Beschwerderecht bei der Behörde

Kontaktdaten des Verantwortlichen

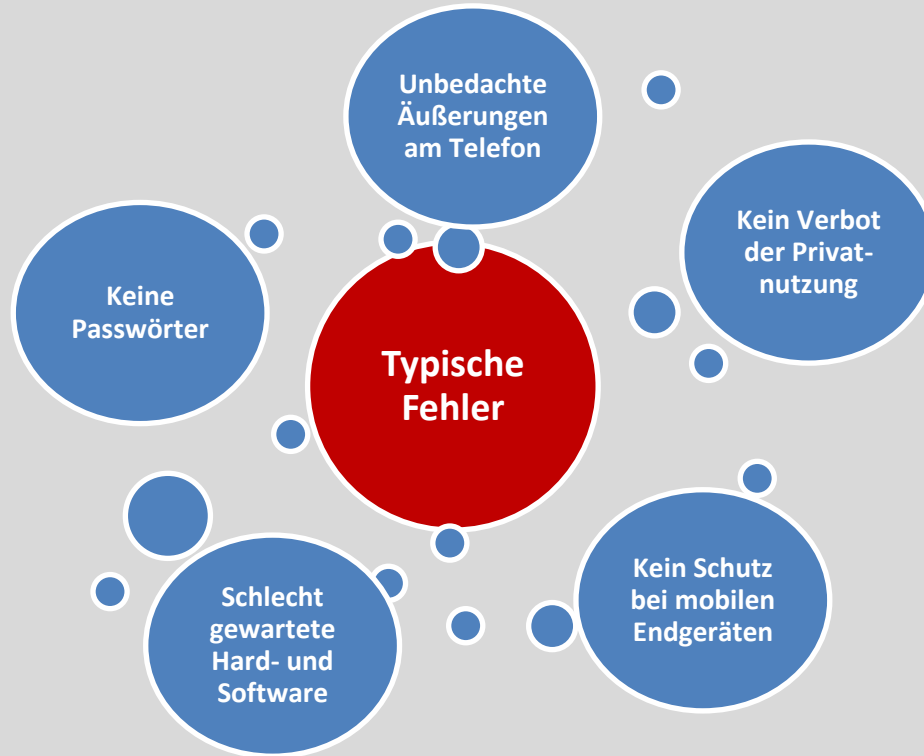


# Schutzpflichten: IT-Sicherheit

- **Art. 32 DSGVO verlangt die Einhaltung eines angemessenen Schutzniveaus.**
- **Dabei sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind.**
- **Gefordert wird Schutz gegen Vernichtung, Verlust, Veränderung sowie unbefugte Offenlegung.**



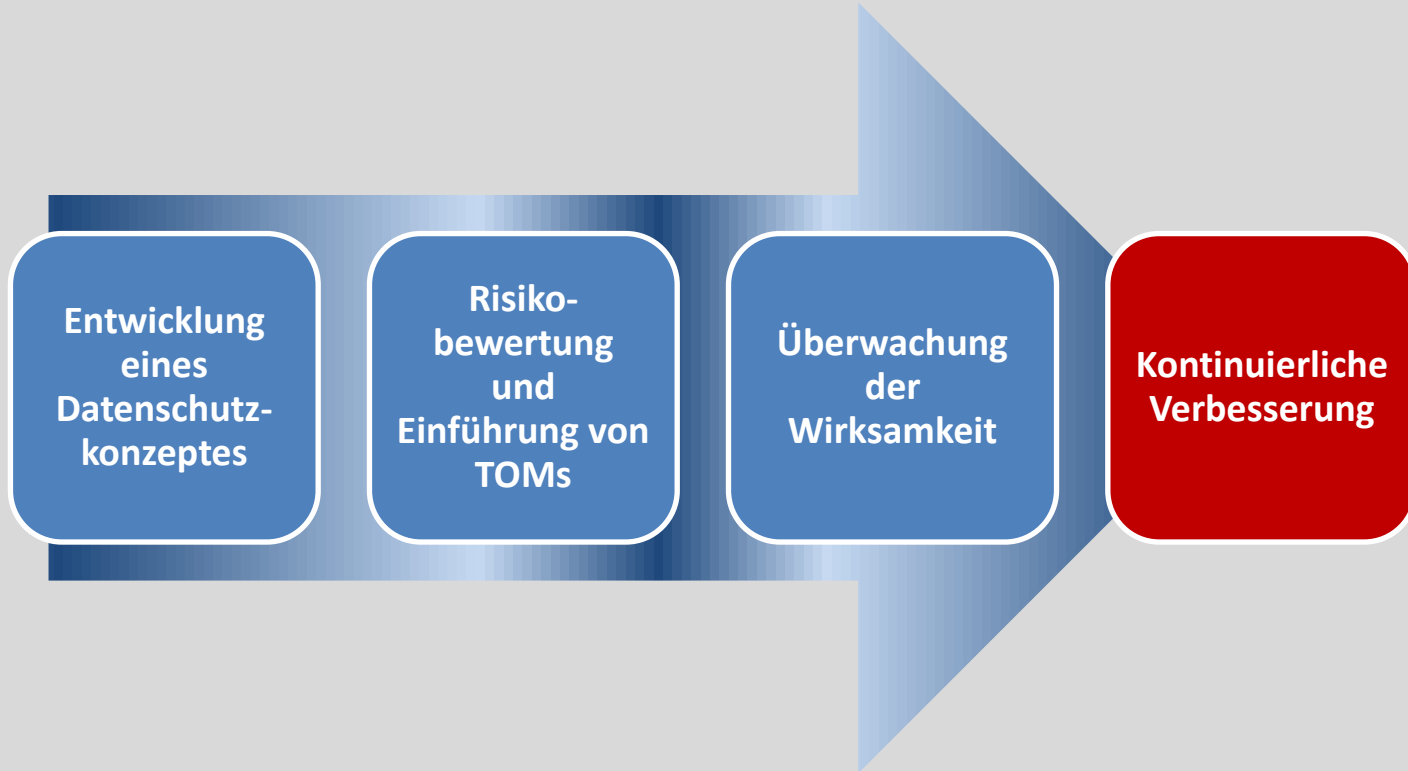
# Typische Fehler







# Einrichtung des Datenschutzkonzepts





## Wann ist ein Datenschutzbeauftragter zwingend zu benennen?

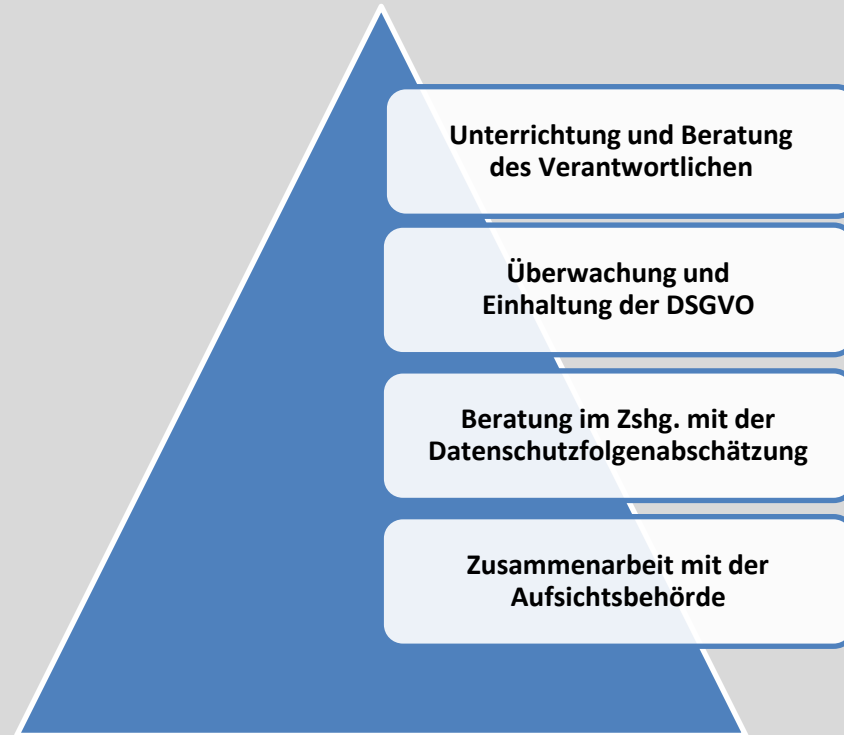
- Soweit mind. 10 MA regelmäßig personenbezogene Daten verarbeiten.
- Wenn der Verantwortliche besonders sensible Daten verarbeitet.



# Aufgaben des Datenschutzbeauftragten

Seite 35

19.05.2018





# Benennung des Datenschutzbeauftragten

Seite 36  
19.05.2018

Die Benennung sollte schriftlich erfolgen!

Datenschutzbeauftragter muss fachlich geeignet sein.

Der Datenschutzbeauftragte berichtet der höchsten Managementebene des Verantwortlichen und hat besonderen Kündigungsschutz.

Kontaktaten sind der Aufsichtsbehörde mitzuteilen.



# Meldepflichten

## Fall:

**RB erfährt, dass Kundendaten gehackt worden sind. Wie soll RB reagieren?**



# Meldepflichten

## *Art. 33 DSGVO:*

*„Im Falle einer Verletzung des Schutzes persönlichen Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Std., nachdem ihm die Verletzung bekannt wurde, diese zuständigen Aufsichtsbehörde.... Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Std., so ist ihr eine Begründung für die Verzögerung beizufügen.“*



# Meldepflichten - Beispiele

Hacking

Verlust

Diebstahl

Fehlversand

Softwarefehler

Fehlentsorgung

Datenausspähung



# Inhalt der Meldung

**Beschreibung der Art der Verletzung/  
Anzahl der Betroffenen**

**Beschreibung der wahrscheinlichen Folgen**

**Beschreibung der ergriffenen Maßnahmen**

**Benennung des Datenschutzbeauftragten**





# Das kommt auf die Unternehmen zu...

Seite 41  
19.05.2018

Prüfpflichten

Informations- und Auskunftspflichten

Dokumentationspflichten

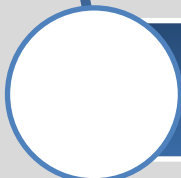


# Das kommt auf die Reisebüros zu...

Seite 42  
19.05.2018



**Meldepflichten**



**Schutzpflichten**



**Organisatorische Pflichten**



# Sofortmaßnahmen...

- **Datenschutzerklärung anpassen!**
- **Verfahrensverzeichnis erstellen!**
- **Auftragsvereinbarung anpassen!**
- **Einwilligungserklärung überprüfen!**
- **Datenschutzbeauftragten bestellen!**
- **Technischen Datenschutz prüfen!**



# Weiterführende Links

[www.lida.Bayern.de](http://www.lida.Bayern.de) (Bay. Landesamt für Datenschutzaufsicht)

[www.lida.niedersachsen.de](http://www.lida.niedersachsen.de) (Nds. Datenschutzbeauftragte)

[www.datenschutz.hessen.de](http://www.datenschutz.hessen.de) (Hess. Datenschutzbeauftragte)

[www.dsgvo-gesetz.de](http://www.dsgvo-gesetz.de)



# Disclaimer

Dieser Vortrag dient der unverbindlichen Information und hat – insbesondere vor dem Hintergrund der sich aktuell noch entwickelnden Rechtslage – keinen Anspruch auf Vollständigkeit und Richtigkeit. Er kann und will auch keine rechtliche Beratung für den Einzelfall ersetzen. Im Zweifel sollte ein Rechtsanwalt / Rechtsanwältin konsultiert werden.



# Vielen Dank für Ihre Aufmerksamkeit!

Seite 46  
19.05.2018

Für die Beantwortung Ihrer Fragen stehe ich Ihnen gern zur Verfügung!



**Dr. jur. Björn Schreier**  
Rechtsanwalt  
Fachanwalt für Handels- und  
Gesellschaftsrecht  
Fachanwalt für Steuerrecht  
dr-schreier@ksh-recht.de

**KAPPUHNE · SCHREIER · HERBOTE**  
PARTNERSCHAFTSGESELLSCHAFT · RECHTSANWÄLTE

Am Münster 28  
37154 Northeim  
Telefon: 05551 / 97 60-0  
Telefax: 05551 / 97 60-50

Düstere-Eichen-Weg 50  
37073 Göttingen  
Telefon: 0551 / 48 862-85  
Telefax: 0551 / 48 862-86

[www.ksh-recht.de](http://www.ksh-recht.de)

Diese Bilder dürfen nur im Zusammenhang mit diesem Vortrag benutzt werden. Copyright KAPPUHNE · SCHREIER · HERBOTE.  
Der Inhalt dieser Präsentation ist urheberrechtlich geschützt und darf nicht vervielfältigt werden.