FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

100 TAGE DSGVO

AUFBRUCH IN DIE DIGITALE ZUKUNFT?

DR. RALF KOLLMANN

Praxity
MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS

INHALT

1. Stand der Dinge – Umsetzung der DSGVO
    1. Aufsichtsbehörden
    2. Unternehmen
    3. Abmahnungen
2. Die Datenschutz-Nachrichten

FIDES
Wir sind Vertrauen.

STAND DER DINGE – UMSETZUNG DER DSGVO

1. Aufsichtsbehörden

FIDES
Wir sind Vertrauen.

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN 1

- **Überlastung der Mitarbeiter**
  - Stark **gestiegene Anzahl von Anfragen und Meldungen** von Datenschutzvorfällen (gegenüber dem Vorjahr voraussichtlich ca. Faktor 2 - 3)
  - Stark **gestiegene Anzahl von Beschwerden** betroffener Personen (gegenüber dem Vorjahr voraussichtlich Faktor 4 - 10, abhängig vom Bundesland)
  - Gestiegene Zahl der Beschwerden geht zu Lasten der verfügbaren Personalkapazitäten für Beratung
  - **Mehraufwand durch Meldeverfahren** für Datenschutzbeauftragte
    - je Bundesland eigenständig und teilweise uneinheitlich durchgeführt
    - führte teilweise zu Abschaltung der Telefone
  - Unklarheit bei rechtlichen Spezialfragen
- Grundsätzlich **Bemühung um Besonnenheit**
- Vereinzelte Aussagen tragen zur **Rechtsunsicherheit** bei (bspw. Paper der DSK zum Umgang mit Web-Tracking)

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN 2

BAYERN

- **Veröffentlichung Ministerratsbeschluss zur DSGVO.** Um der Angst – und der Neugierde – vor dem ersten Bußgeld nach Art. 83 DSGVO zu begegnen, stellt der Ministerratsbeschluss fest, dass bei einem Erstverstoß die Beratung und Hinweise an erster Stelle stehen werden.
- **Handreichungen des BayLDA** für kleine Unternehmen und Vereine
- Informationspapiere zu zahlreichen Themen der DSGVO

HAMBURG

Beschwerdeformular zum EU-US Privacy Shield ist online

- Haben Sie Dienstleister in den USA / Drittländern? **Sind Sie sicher?**
- Auf welcher Rechtsgrundlage erfolgt bei Ihnen die Verarbeitung?

LDI NRW

Unterlassene Meldungen des bDSB werden bis zum 31.12.2018 nicht als Datenschutzverstöße verfolgt.

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN

NIEDERSACHSEN

- **Anlasslose Prüfung** in 50 Unternehmen
- Ziel ist die **Orientierung** über die Umsetzung der DSGVO
- **„Es geht zum jetzigen Zeitpunkt nicht vorrangig darum, möglichst viele Fehler zu finden und Bußgelder zu verhängen.“**
- **„Trotzdem kann es natürlich zu einem entsprechenden Verfahren kommen, wenn wir während der Prüfung Verstöße gegen die DSGVO feststellen.“**

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN 4

NIEDERSACHSEN

- **Prüfungsinhalte**
  - Status der Vorbereitung auf die DSGVO
  - Verzeichnis der Verarbeitungstätigkeiten
  - Zulässigkeit der Verarbeitung
  - Betroffenenrechte
  - Technischer Datenschutz
  - Datenschutz-Folgenabschätzung
  - Auftragsverarbeitung
  - Datenschutzbeauftragter
  - Meldepflichten
  - Dokumentation

- Vergleichbare Prüfungen durch Aufsichtsbehörden anderer Bundesländer werden voraussichtlich zukünftig erfolgen.

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN

LISTE DER DATENSCHUTZ-FOLGENABSCHÄTZUNGEN (DSF)

- Die Datenschutz-Aufsichtsbehörden haben festgelegt, bei welchen Datenverarbeitungen obligatorisch eine DSF durchzuführen ist.

- Eine **Liste von Verarbeitungsvorgängen** nach Art. 35 Abs. 4 DSGVO (Datenschutz-Folgenabschätzung) ist veröffentlicht.

LISTE DER DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

Kriterien zur Einordnung von Verarbeitungsvorgängen (WP 248 der Artikel-29-Datenschutzgruppe)

1. Bewerten oder Einstufen (**Scoring**)
2. Automatisierte **Entscheidungsfindung** mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische **Überwachung**
4. **Vertrauliche** oder höchst persönliche Daten
5. Datenverarbeitung in **großem Umfang**
6. Abgleichen oder **Zusammenführen** von Datensätzen
7. Daten zu **schutzbedürftigen** Betroffenen
8. **Innovative Nutzung** oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. **Betroffene werden** an der **Ausübung eines Rechts** oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags **gehindert**

LISTE DER DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

- **Kriterien zur Durchführung der Datenschutz-Folgenabschätzung**
  - Zwei oder mehr Kriterien treffen auf ein Verfahren zu → DSF obligatorisch
  - Ein Kriterium trifft zu → DSF zu prüfen
  - Kein Kriterium trifft zu und hohes Risiko für Betroffene besteht (auch nicht in der Liste genannte Risiken) → DSF zu prüfen

- Die DSF sollte immer mit einer **dokumentierten Eingangsprüfung** zur Beurteilung bestehender Risiken begonnen werden.
- Die **Verantwortung für die Risikoeinschätzung** und Durchführung erforderlicher DSF liegt bei der verantwortlichen Stelle.
- Der Datenschutzbeauftragte berät und unterstützt (auf Anfrage) und überwacht ihre Durchführung (letzteres auch ohne Anfrage).

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN 8

LISTE DER DATENSCHUTZ-FOLGENABSCHÄTZUNGEN – BEISPIELE 1

- **Umfangreiche Verarbeitung von Daten über den Aufenthalt von Personen**
  - Car Sharing / Mobilitätsdienste
  - Kundenbewegung in Kaufhäusern / Einkaufszentren
  - Telemetriedaten / GPS-Ortung im Firmenfahrzeug
- **Umfangreiche Verarbeitung von Daten über das Verhalten von Personen**
  - Verwendung von Kundenkarten / Analyse des Einkaufsverhaltens
- **Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen**
  - Big Data / Data Mining / Profilbildung bzw. Analyse des Verhaltens – auch pseudonymisiert
  - Fraud Prevention
  - Scoring bspw. durch Auskunfteien, Banken, Versicherungen

STAND DER DINGE – UMSETZUNG DER DSGVO

AUFSICHTSBEHÖRDEN 9

LISTE DER DATENSCHUTZ-FOLGENABSCHÄTZUNGEN – BEISPIELE 2

- **Verhaltens- und Leistungskontrolle von Beschäftigten**
  - Beobachtung anhand von Protokolldaten
  - Auswertung der Internetnutzung
- **Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten**
  - Bspw. automatisierte Auswertung der Stimmungslage durch Callcenter
- Verarbeitung von Daten, die einem **Sozial-** oder **Berufsgeheimnis** unterliegen

STAND DER DINGE – UMSETZUNG DER DSGVO

2. Unternehmen

FIDES
Wir sind Vertrauen.

STAND DER DINGE – UMSETZUNG DER DSGVO

UNTERNEHMEN

GESTIEGENE RISIKO- UND PROBLEMWAHRNEHMUNG

- Wahrgenommene **Belastung** durch die Umsetzung
- Veränderte **Risikowahrnehmung**, insbesondere durch die Änderung der Bußgelder
- **Rechtsunsicherheit** und Unkenntnis führen zu Problematisierung und **fehlender Differenzierung** zwischen kritischen und harmlosen Sachverhalten, bspw.
  - Problematisierung des Umgangs mit Visitenkarten
  - Problematisierung von harmlosen Sachverhalten (bspw. Aufruf im Wartezimmer)
  - Ausnutzung von Unkenntnis ("Einwilligungsfischerei" für Werbung)

STAND DER DINGE – UMSETZUNG DER DSGVO

UNTERNEHMEN 2

POSITIVE ASPEKTE DER UMSETZUNG

- Dokumentationspflichten (bspw. Verfahrensverzeichnis und Art. 13) ermöglichen eine **Verbesserung der Prozess-Transparenz** im Unternehmen
- Geschäftsführung und Management werden – im positiven Sinne – gezwungen, sich mit den bestehenden **Geschäftsprozessen**, der darin erfolgenden Datenverarbeitung und dessen Erfordernis **auseinanderzusetzen**
  - Sind die Prozesse noch aktuell bzw. erforderlich?
  - Wird die Datenverarbeitung überhaupt benötigt?
  - Haben zuviele bzw. die richtigen Mitarbeiter Zugriff?
  - Werden nicht benötigte Datenkategorien verarbeitet?

STAND DER DINGE – UMSETZUNG DER DSGVO

UNTERNEHMEN

ES BESTEHT NACH WIE VOR HANDLUNGSBEDARF

- Fehlende Identifizierung und Beurteilung der bestehenden **Schutzmaßnahmen** in Unternehmen
- Fehlende Identifizierung und Beurteilung von (relevanten) **Risiken**
- **Datenschutzfolgenabschätzungen** in vielen Unternehmen weder identifiziert noch durchgeführt
- Behandlung **tatsächlicher Datenschutzprobleme** bleibt bisher oft unerkannt oder wird ignoriert
- Wirksames **Datenschutz-** und **IT-Sicherheitsmanagement** in vielen Unternehmen noch nicht eingeführt

DOKUMENTATION VON "TOMS" GENÜGT NICHT:

- **Angemessenheit** der Maßnahmen (hinsichtlich identifizierter Risiken) prüfen
- **Maßnahmen** ggf. anpassen bzw. ergänzen
- Als Maßstab dient der **"Stand der Technik":**
  - Turnusmäßige Prüfungen erforderlich
  - kontinuierliche Weiterentwicklung erforderlich (s.o.)

STAND DER DINGE – UMSETZUNG DER DSGVO

EXKURS: TECHNISCHER DATENSCHUTZ

STAND DER TECHNIK – WAS IST DAS? 1

- Da die **technische Entwicklung schneller ist als die Gesetzgebung**, hat es sich bewährt, in Gesetzen den Begriff "Stand der Technik" zu verwenden, statt zu versuchen, konkrete technische Anforderungen festzulegen.
- Weder in der DSGVO noch im IT-Sicherheitsgesetz abschließend definiert.
  - "Die im Waren- und Dienstleistungsverkehr **verfügbaren Verfahren**, Einrichtungen oder Betriebsweisen, deren Anwendung die **Erreichung der** jeweiligen **gesetzlichen Schutzziele** am **wirkungsvollsten gewährleisten** kann."

    "Handreichung zum Stand der Technik" des Bundesverband IT-Sicherheit e.V. (TeleTrusT):
  - **"**Organisatorische und technische Vorkehrungen gelten dann als angemessen, **wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen steht**, die ein Ausfall oder eine Beeinträchtigung der betroffenen Kritischen Infrastruktur hätte."

    Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/B3S/b3s_node.html (12.09.2018)

- Faktisch geprägt durch technische Standards, Empfehlungen (bspw. BSI) und faktischen Einsatz von Technologie.

STAND DER DINGE – UMSETZUNG DER DSGVO

EXKURS: TECHNISCHER DATENSCHUTZ

BEISPIEL ZUR ENTWICKLUNG DES STANDES DER TECHNIK

- **Informationssicherheitsbeauftragter**
  - BSI fordert ISB im "Leitfaden Basisabsicherung" – genügt das?
- **Verschlüsselung**
  - **Whatsapp** (1 Mrd. Menschen nutzen allein hier täglich Ende-zu-Ende-Verschlüsselung)
  - **HTTPS** (Verschlüsselung der Webpräsenz – § 13 Abs. 7 TMG verweist auf SdT)
  - **TLS**
    - TeleTrusT: "Handreichung zum Stand der Technik"
    - BSI: Mindeststandard für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden
    - BSI: Grundschutzkompendium 2018
- **BSI: Empfehlung zu Schlüssellängen** *(BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen)*
  - Aktuelle Empfehlungen gelten bis 2024 (das Dokument wird jährlich aktualisiert)

  Für welchen **Zeitraum** sollen Inhalte vertraulich sein? Beispiel RSA:
    - bis 2022: 2000 Bit
    - ab 2023: 3000 Bit

STAND DER DINGE – UMSETZUNG DER DSGVO

3. Abmahnungen

FIDES
Wir sind Vertrauen.

STAND DER DINGE – UMSETZUNG DER DSGVO

ABMAHNUNGEN 1

ABMAHNWELLE

- Die befürchtete große **Abmahnwelle** ist weitgehend ausgeblieben.
- Abmahnungen im Zusammenhang mit der DSGVO traten gleichwohl auf:
  - Fehlende oder nicht an die DSGVO angepasste **Datenschutzerklärungen** (Web)
  - Verwendung von Google Maps und Google Web Fonts
  - **Fehlende Verschlüsselung** von Webverbindungen (fehlende SSL-Zertifikate)
- Ob bzw. in welcher Form die Vorschriften der DSGVO überhaupt abgemahnt werden können, wird gegenwärtig in Fachkreisen kontrovers diskutiert.
- Bis auf Weiteres sollte davon ausgegangen werden, dass Abmahnungen weiterhin möglich sind.

STAND DER DINGE – UMSETZUNG DER DSGVO

ABMAHNUNGEN 2

MISSBRÄUCHLICHE ABMAHNUNGEN

- In manchen Fällen erscheinen die erfolgten Abmahnungen **dubios** und deren **Zulässigkeit fragwürdig.**
- Seitens der CDU/CSU-Bundestagsfraktion wurde ein – zumindest vorübergehendes – gesetzliches **Verbot von Abmahnungen** gefordert (bisher jedoch erfolglos).
- Gesetzliche Maßnahmen gegen **missbräuchliche Abmahnungen** sind weiterhin im Gespräch.
- **Gegen-Abmahnungen** wegen "rechtsmissbräuchlicher Abmahnung" sind bereits in Einzelfällen erfolgt.

DIE DATENSCHUTZ-NACHRICHTEN

DIE DATENSCHUTZ-NACHRICHTEN

… EUROPA…

ÖSTERREICH VERSCHIEBT E-PRIVACY-VERORDNUNG

In ihrer Funktion als Ratsvorsitzende der Europäischen Union plant die Österreichische Regierung offenbar eine **Verschiebung der E-Privacy-Verordnung**. Sollte sich dies verwirklichen, ist mit einer Verabschiedung erst frühestens 2020 zu rechnen.

UK

"Im **Datenskandal um Cambridge Analytica** kündigen die Ermittler ein Bußgeld von 500.000 Pfund an. Kein riesiger Betrag, denn die Verfehlungen fielen in die Zeit vor der Datenschutzgrund-verordnung. Die Briten wollen künftig strenger gegen den Missbrauch von Nutzerdaten bei politischer Werbung vorgehen." (Quelle: Netzpolitik.org)

Erste Anzeichen ergeben, dass **Großbritannien** auch **nach dem Brexit** die DSGVO einhalten will.

EU

Die EU-Abgeordneten des Innenausschusses (LIBE) haben die EU-Kommission aufgefordert, beim **Privacy-Shield**-Abkommen **nachzubessern** oder dieses auf Eis zu legen.

DIE DATENSCHUTZ-NACHRICHTEN

… UND INTERNATIONAL..

USA

Die USA arbeiten gegenwärtig an einem neuen **Datenschutzgesetz**, welches "nicht so aggressiv wie die DSGVO" sein soll.

Bereits im März hatte die US-Regierung durch die Veröffentlichung des **US Cloud Act** ("Clarifying Lawful Overseas Use of Data Act") bei europäischen IT-Dienstleistern für Verunsicherung gesorgt. Die Möglichkeiten von nach Europäischem Recht datenschutzkonformen Datentransfers zwischen EU und USA werden dadurch erschwert.

BRASILIEN

Brasilien veröffentlichte kürzlich ein eigenes Datenschutzgesetz.

Der Umfang und die vom brasilianischen Gesetzgeber vorgesehenen Regelungen erinnern stark an die Datenschutz-Grundverordnung. Eine **gegenseitige Anerkennung** des ab 2020 geltenden Gesetzes mit der EU ist denkbar.

JAPAN

Im Zuge des neuen Freihandelsabkommens zwischen der EU und Japan (JAFTA) will die EU das japanische Datenschutzsystem (APPI, zuletzt 2015 reformiert), durch einen **Angemessenheitsbeschluss** der EU-Kommission, als gleichwertig anerkennen.

WERBUNG

1. …nur ein Werbespot … bleiben Sie dran!

FIDES
Wir sind Vertrauen.

KOMPAKTKURS DATENSCHUTZBEAUFTRAGTER (DSGVO)

SEMINARANKÜNDIGUNG

Seminarschwerpunkte

- Pflichten des betrieblichen Datenschutzbeauftragten
- Dokumentations- und Nachweispflichten
- Verzeichnis der Verarbeitungstätigkeiten
- Konzeption des Datenschutz-Managementsystems
- Auftragsverarbeitung
- Werbung
- Arbeitnehmerdatenschutz / Kundendatenschutz
- Technischer Datenschutz und IT-Sicherheitsmanagement

Datum: **6. – 9. November 2018**

Ort: **Seminarräume der FIDES**

Niederlassung Bremen, Birkenstraße 37

NOCH FRAGEN?

EIN GESPRÄCH BEWEGT MEHR. IHR ANSPRECHPARTNER.

Dr. Ralf Kollmann

POSITION BEI FIDES	Bereichsleiter Datenschutzberatung / Senior Manager
KONTAKTDATEN	Telefon: +49 (421) 3013-408 E-Mail: r.kollmann@fides-online.de
KURZVITA	• Seit 2005 bei der FIDES IT Consultants GmbH • Zertifizierter Datenschutzbeauftragter (TÜV ©) • Bereichsleiter Migrationsprojekte bei der BOSS AG, Bremen • Wissenschaftlicher Mitarbeiter am Lehrstuhl Datenbanksysteme der Universität Bremen • Systemadministrator beim Institut für Seeverkehrswirtschaft und Logistik, Bremen
QUALIFIKATION	• Diplom-Informatiker • Diplom-Wirtschaftsinformatiker (Studienschwerpunkt Unternehmensrecht) • Dr.-Ing. (Promotion im Bereich Softwaretechnik und Datenbanksysteme)
RELEVANTE ERFAHRUNGEN / TÄTIGKEITSSCHWERPUNKTE	• Analyse und Beratung in den Bereichen Datenschutz, IT-Compliance und IT-Sicherheit • Beratung bei der Gestaltung und Einführung von Datenschutz-Management-Systemen • Prüfung von IT-Systemen, IT-Verfahren und IT-gestützten Prozessen nach nationalen und internationalen Rechnungslegungs- und Prüfungsstandards (bspw. IDW PS/ PH/FAIT, ISA, SAS) • Projektmanagement und Projektcontrolling in IT-Projekten • Konzeption und Leitung der Qualitätssicherung in Software-Entwicklungsprojekten

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

FIDES TREUHAND GMBH & CO. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

HAUPTNIEDERLASSUNG
Birkenstraße 37
28195 Bremen
Postfach 10 57 27
28057 Bremen
Telefon +49 (421) 3013-0
Fax +49 (421) 3013-100
bremen@fides-online.de
www.fides-online.de

ZWEIGNIEDERLASSUNGEN
Hamburg
Hannover
Bremerhaven
Osnabrück
Düsseldorf
Leer
Berlin
Rostock

FIDES IT CONSULTANTS GMBH

HAUPTNIEDERLASSUNG
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-400
Fax +49 (421) 3013-449
bremen@fides-online.de
www.fides-online.de

ZWEIGNIEDERLASSUNG
Hamburg

FIDES FINANCIAL SERVICES GMBH
Wirtschaftsprüfungsgesellschaft
Darmstädter Landstraße 108
60598 Frankfurt am Main
Telefon +49 (69) 9622-0498
Fax +49 (69) 9622-0420
frankfurt@fides-online.de
www.fides-online.de

FIDES CORPORATE FINANCE GMBH
Wirtschaftsprüfungsgesellschaft
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-0
Fax +49 (421) 3013-100
bremen@fides-online.de
www.fides-online.de

NÖLLE & STOEVESANDT
Rechtsanwälte
Partnerschaftsgesellschaft
Birkenstraße 37
28195 Bremen
Telefon +49 (421) 3013-165
Telefax +49 (421) 3013-166
info@noelle-stoevesandt.de
www.noelle-stoevesandt.de