HERZLICH WILLKOMMEN.

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer

Steuerberater

IT-Berater

Unternehmerberater

Nölle & Stoevesandt Rechtsanwälte

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

ENDSPURT ZUR DSGVO – WIE UNTERNEHMEN PRIORISIEREN SOLLTEN

DR. RALF KOLLMANN

Düsseldorf, 20. Februar 2018

Praxity MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS

INHALT

EINLEITUNG

Hintergrund zur DSGVO

EINLEITUNG

HINTERGRUND ZUR DSGVO

ZIELE

- **HARMONISIERUNG:** Durch die DSGVO soll ein einheitliches Datenschutzrecht für alle EU-Mitgliedsstaaten realisiert werden.
- **NATIONALE SONDERREGELUNGEN** sollen vermieden bzw. reduziert werden.
- Der **WANDEL ZUR DIGITALEN GESELLSCHAFT** mit stetig steigenden Anforderungen an den Datenschutz soll berücksichtigt werden.

WAS ÄNDERT SICH?

- **UNMITTELBARKEIT:** Die DSGVO gilt als Verordnung unmittelbar in jedem Mitgliedsstaat von Europa, ohne dass sie in nationales Recht umgewandelt werden muss.
- **VORRANG:** Sie gilt zukünftig vorrangig vor dem nationalen Recht (Kehrtwende zum alten BDSG als subsidiärer Rechtsnorm).
- **ÖFFNUNGSKLAUSELN** bieten nationalen Gesetzgebern die Möglichkeit, eigene nationale Regelungen in Form von Anpassungsgesetzen zu erlassen.
- In Deutschland wird vor diesem Hintergrund das **NEUE BUNDESDATENSCHUTZGESETZ** am 25. Mai 2018 in Kraft treten.

EINLEITUNG

HINTERGRUND ZUR DSGVO

MARKTORTPRINZIP

- Der **GELTUNGSBEREICH** der DSGVO wird erweitert. Er erfasst nicht nur den EU-Raum, sondern auch Unternehmen, die
  - in der EU tätig sind (selbst oder durch Niederlassungen)
  - in der EU Waren oder Dienstleistungen anbieten (bspw. Online-Shop in den USA, aber auch kostenlose Leistungen)
  - das Verhalten von Personen in der EU beobachten (bspw. Webshops, Content-Provider, Google, Facebook, diverse Apps)

EINLEITUNG

HINTERGRUND ZUR DSGVO

WESENTLICHE PARADIGMEN

- **VERBOT MIT ERLAUBNISVORBEHALT:** Rechtsgrundlagen der Verarbeitung werden wichtiger.
- **TRANSPARENZ:** Informations- und Hinweispflichten gewinnen an Bedeutung.
- **ZWECKBINDUNG:** Die Verarbeitung darf nur zu dem bei der Erhebung festgelegten, legitimierten Zweck erfolgen.
- **RICHTIGKEIT:** Die Korrektheit und Integrität der Daten muss gewährleistet werden.
- **PRIVACY BY DESIGN:** Die Berücksichtigung des Datenschutzes muss bereits bei der Konzeption, d.h. vor Inbetriebnahme von Verfahren, erfolgen.
- **PRIVACY BY DEFAULT:** Etwaige Voreinstellungen müssen datenschutzfreundlich eingestellt sein.
- **SPEICHERBEGRENZUNG:** Die Erhebung personenbezogener Daten soll auf das dem Zweck nach erforderliche Minimum reduziert sein.
- **NACHWEISBARKEIT / RECHENSCHAFTSPFLICHT:** Die Einhaltung des Datenschutzes muss sowohl bei der Durchführung als auch bei der Konzeption der Verfahren nachvollziehbar dokumentiert werden. Die Dokumentationspflichten werden **DEUTLICH ERWEITERT**.

EINLEITUNG

DAS NEUE BUNDESDATENSCHUTZGESETZ

- Das neue **BUNDESDATENSCHUTZGESETZ** ergänzt zukünftig die DSGVO auf nationaler Ebene in Deutschland.
- Die Struktur ist gegenüber den alten, bis zum 24. Mai 2018 geltenden Bundesdatenschutzgesetz grundlegend verändert.
- Das neue Gesetz dient der Umsetzung von **ÖFFNUNGSKLAUSELN** der DSGVO.

STRUKTURELLER AUFBAU

- Das neue Bundesdatenschutzgesetz ist in **VIER TEILE** gegliedert.
- Teile 1, 2 und 4 sind für die meisten Unternehmen relevant (§§ 1 – 44 und 85 BDSG-neu)
- **WAS IST MIT TEIL 3?**
  - "Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680".
  - Verarbeitung für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten.
  - Im wörtlichen Sinn für die meisten Unternehmen nicht einschlägig.
  - Eine mögliche Ausstrahlungswirkung wird in Fachkreisen diskutiert – Rechtsunsicherheit ist absehbar.
  - Die Umsetzung der Regelungen aus Teil 3 sollte im Einzelfall geprüft werden.

ENDSPURT ZUR DSGVO

Priorisierte Umsetzung der DSGVO

PRIORISIERTE UMSETZUNG DER DSGVO

PRIORITISATION IN A NUTSHELL

PRIORISIERUNG BEDEUTET NICHTS ANDERES ALS DAS FESTLEGEN EINER RANGFOLGE ZU ERLEDIGENDER AUFGABEN

- Die vorgestellten Datenschutz-Themen stellen einen **EXEMPLARISCHEN KERN** relevanter Tätigkeiten bei der Umsetzung der DSGVO dar.
- Diverse **ANDERE PFLICHTEN** im Datenschutz sind ebenfalls relevant und in vielen Fällen bußgeldbehaftet oder durch andere Risiken relevant.
- Die hier vorgenommene Priorisierung muss – abhängig von dem je Unternehmen individuellen Beurteilungsmaßstab – nicht auf jedes Unternehmen gleichermaßen zutreffen.

WIE WIRD PRIORISIERT?

Im jedem Unternehmen individuell festzulegen sind:

- Die **STRATEGISCHE AUSRICHTUNG** von Datenschutz und IT-Sicherheit.
- Abgeleitet daraus die Kriterien / **DER BEURTEILUNGS-MAßSTAB** für datenschutzrechtliche und unternehmerische Risiken.
- Die eigene **RISIKOEINSTELLUNG.**
- Dies dient als Grundlage bei der **PLANUNG** Ihres DSGVO-Projekts.

DATENSCHUTZ-MANAGEMENTSYSTEM

Strategie und Konzeption des Datenschutzes

DATENSCHUTZ-MANAGEMENTSYSTEM

INHALT UND EBENEN

STRATEGIE

- **RELEVANZ** des Datenschutzes im Unternehmen.
- **VERFOLGTE ZIELE** bei der Umsetzung des Datenschutzes (bspw. Compliance, USP, Schutz von Unternehmenswerten).
- **KRITIKALITÄT** von Datenschutz und IT-Sicherheit im Unternehmen.

KONZEPTION

- Zentrale **LEITLINIEN** für die Umsetzung des Datenschutzes.
- Konkretisierte konzeptionelle **AUSGESTALTUNG** der datenschutzrechtlichen Pflichten und Verfahren.
- Erstellung von **ARBEITSDOKUMENTEN** (Nachvollziehbarkeit von Konzeption und Durchführung).

KONTROLLEN

- Zentrale **VERANKERUNG** des Datenschutzes im Unternehmen.
- **EINBETTUNG** des Datenschutzes im Risikomanagement bzw. im internen Kontrollsystem.
- **AUFBAU VON KONTROLLEN**, welche die Angemessenheit der getroffenen Schutzmaßnahmen dauerhaft sicherstellen und Handlungsbedarfe zuverlässig aufdecken.

DATENSCHUTZ-MANAGEMENTSYSTEM

VORGEHEN

ZENTRALE FRAGEN

- In welchen **GESCHÄFTSPROZESSEN** werden personenbezogene Daten verarbeitet?
- Um welche **ART VON DATEN** handelt es sich?
- Wer ist **BETROFFEN**?
- **WO** erfolgt die Datenverarbeitung
  - auf sachlicher Ebene (IT-Systeme)
  - auf gesellschaftlicher Ebene (Konzern, Dienstleister)
  - auf räumlicher Ebene (Dezentralisierung / Ausland)
- Welche **NORMATIVEN VORGABEN** zur Verarbeitung bestehen?
- Wie sind die Daten geschützt? Ist der **SCHUTZ ANGEMESSEN**?

DATENSCHUTZ-MANAGEMENTSYSTEM

VORGEHEN

VORGEHEN

- Festlegung der **STRATEGISCHEN AUSRICHTUNG** (Soll)
- Prozess- und **SYSTEMAUFNAHME** (Ist)
- Ggf. Durchführung einer separaten **PRÜFUNG DER IT-SICHERHEIT**
- **GAP-ANALYSE**
- **PLANUNG** (Datenschutz-Planung ist IT-Projektmanagement)
- **KONZEPTION** des Datenschutz-Managementsystems
- **UMSETZUNG**
  - **TECHNISCHE MAßNAHMEN** (bspw. zentrale Software-Updates, Verschlüsselung, Firewalls, Anti-Virus)
  - **ORGANISATORISCHE MAßNAHMEN** (bspw. Datenschutz-Richtlinien, Betriebsvereinbarungen, Dienstanweisungen, Verschwiegenheitsverpflichtungen)
  - Ggf. **ANPASSUNG** von Verfahren
- Turnusmäßige und anlassbezogene Durchführung von **KONTROLLEN**
- Einbettung in **QS-ZYKLUS** (Plan – Do – Check – Act)

BETROFFENENRECHTE

Schutz von Persönlichkeitsrechten

BETROFFENENRECHTE

TRANSPARENZPFLICHTEN

INFORMATIONSPFLICHTEN

- Informierung zum Zeitpunkt
  - der **DATENERHEBUNG**
  - des **EMPFANG**s der Daten von Dritten
  - der **ANSPRACHE** eines Kunden
- Der **UMFANG** der Informationspflichten wurde ggü. dem BDSG-alt **DEUTLICH ERWEITERT.**

WIDERSPRUCHS- UND WIDERRUFSRECHTE

- Zu berücksichtigen sind
  - **WIDERRUFSRECHTE** bei erteilter Einwilligung sowie
  - generelle **WIDERSPRUCHSRECHTE** in Abhängigkeit von der Art der Datenverarbeitung
- Auch hier ist eine **DEUTLICHE ERWEITERUNG** erfolgt.
- Zu berücksichtigen u.a. bei **WERBUNG**, **PROFILING** und jeder auf **BERECHTIGTES INTERESSE** gestützten Verarbeitung.
- Widerspruchs- und Widerrufsrechte sind ebenfalls mit einer Informationspflicht verbunden.
- Systematische **INVENTARISIERUNG** aller einschlägigen Fälle empfehlenswert.

BETROFFENENRECHTE

RICHTIGKEIT, INTEGRITÄT UND ZUGRIFF

BERICHTIGUNG, LÖSCHUNG UND EINSCHRÄNKUNG

- Diese Betroffenenrechte sind grundsätzlich dem BDSG-alt bekannt:
  - **BERICHTIGUNG** falscher Daten
  - **LÖSCHUNG** personenbezogener Daten nach Wegfall des Verwendungszwecks (und gesetzlicher Aufbewahrungsfristen)
  - **EINSCHRÄNKUNG** des Zugriffs auf Daten, bspw. weil diese (noch) nicht gelöscht werden dürfen (u.a. Aufbewahrungsfristen, Verteidigung von Rechtsansprüchen)
- Der Begriff der Einschränkung (ehemals Sperrung) wurde deutlich erweitert.
- Die Erstellung einer zweistufigen **LÖSCHKONZEPTION** ist empfehlenswert.

KASKADIERUNG

- **PFLICHT ZUR INFORMIERUNG** aller Daten-Empfänger über jede Einforderung der obigen Rechte.
- Die Empfänger sind verpflichtet, die eingeforderten Rechte in gleicher Weise umzusetzen und ihrerseits eine **INFORMIERUNG ALLER EMPFÄNGER** zu veranlassen.

BETROFFENENRECHTE

DATENANALYSEN

AUTOMATISIERTE EINZELENTSCHEIDUNGEN UND PROFILING

- Automatisierte, datenbasierte Entscheidungen, welche
  - **RECHTSWIRKUNG** für den Betroffenen entwickeln (können) oder
  - in "ähnlicher Weise" zu **ERHEBLICHEN BEEINTRÄCHTIGUNGEN** führen können
- Analysen personenbezogener Daten, welche eine **BEURTEILUNG** oder **VORHERSAGE** des Verhaltens zum Ziel haben.
- **EINGESCHRÄNKTE ZULÄSSIGKEIT** – Die Voraussetzungen sind sorgfältig zu prüfen.

DATA MINING / BIG DATA

- **ANWENDUNG MATHEMATISCHER VERFAHREN** auf große Datenmengen, um neue Muster und Zusammenhänge zu erkennen.
- Oft werden hierzu **VERSCHIEDENE DATENQUELLEN** zusammengeführt.
- Verstöße gegen das **TRENNUNGSGEBOT**, **DATENMINIMIERUNG** und Bestehen einer **RECHTSGRUNDLAGE** ("Änderung des Zwecks der Verarbeitung") sind zu prüfen.
- Separate **INFORMATIONSPFLICHT.**
- Erfordernis weiterer **DATENSCHUTZKONTROLLEN** (bspw. **ANGEMESSENHEIT** getroffener Schutzmaßnahmen, Datenschutz-Folgenabschätzung) zu prüfen.

BETROFFENENRECHTE

AUSKÜNFTE UND DATENEXPORT

AUSKUNFTSRECHT

- Recht der betroffenen Person, **AUSKUNFT** über und eine **KOPIE** ihrer gespeicherten Daten zu verlangen.
- Das Recht umfasst die Auskunft über die Daten (im gesetzlich festgelegten Umfang) und die Bereitstellung der Kopie.

DATENMOBILITÄT

- Recht der betroffenen Person, alle sie betreffenden, von ihr bereitgestellten personenbezogenen Daten in einem
  - strukturierten
  - gängigen
  - maschinenlesbaren

Format zu erhalten.

- Die "Bereitstellung" kann sowohl aktiv als auch passiv erfolgt sein.
- Das Recht umfasst die Übermittlung der Daten an die betroffene Person oder eine von ihr genannte Stelle.

BETROFFENENRECHTE

FAZIT

- Die Umsetzung der Rechte betroffener Personen kann mit einem **ERHEBLICHEN AUFWAND** verbunden sein – sowohl in der Vorbereitung als auch der Umsetzung.
- Eine sorgfältige und **FRÜHZEITIGE PRÜFUNG** sollte im Unternehmen individuell durchgeführt werden:
  - Welche Personen-Gruppen sind zu berücksichtigen (Mitarbeiter, Kunden etc.)?
  - Wie ist die **GRÖßENORDNUNG ZU ERWARTENDER ANFRAGEN** einzuschätzen?
  - Welche Betroffenenrechte sind in besonderem Maße zu berücksichtigen?
  - Welche Daten sind jeweils bereitzustellen?
- Basierend darauf sollte individuell festgelegt werden,
  - wie die **AUSGESTALTUNG** der Betroffenenrechte im Unternehmen erfolgt
  - welche **VORBEREITUNGEN** jeweils zu treffen sind
- Die Vorbereitung sollte auch die Festlegung der **EINGANGSVORAUSSETZUNGEN** zur Geltendmachung berücksichtigen, bspw.
  - Identifizierbarkeit der Person / Zweifel an der Identität
  - ggf. Vorliegen einer Vollmacht
  - "offenkundig unbegründete" Anträge / exzessive Anträge

AUFTRAGSVERARBEITUNG

Datenschutzkonforme Beauftragung von Dienstleistern

AUFTRAGSVERARBEITUNG

DATENSCHUTZKONFORME BEAUFTRAGUNG VON DIENSTLEISTERN

UNVERÄNDERT…

Wesentliche **PFLICHTEN DES AUFTRAGGEBERS** bleiben erhalten, bspw.

- Verpflichtung zur vertraglichen Regelung
- Sorgfältige Auswahl von Auftragnehmern ("Garantien")
- Kontrollpflicht angemessener Schutzmaßnahmen beim Dienstleister

… UND VERÄNDERT

- Die vorgeschriebenen **INHALTE DER VERTRAGLICHEN REGELUNG** wurden in der DSGVO erweitert, bspw. "dokumentierte Weisungen" und Umgang mit Subunternehmern.
- Erweitertes **HAFTUNGSRISIKO FÜR AUFTRAGNEHMER** (gesamtschuldnerische Haftung).

NEUE OPTIONEN

- **GEMEINSAME VERARBEITUNG**, bspw. als Option bei Konzern-Datenverarbeitung
- **VERARBEITUNG IM KONZERN** ("kleines" Konzernprivileg, Art. 28 i.V.m. EG 48 DSGVO)

AUFTRAGSVERARBEITUNG

DATENSCHUTZKONFORME BEAUFTRAGUNG VON DIENSTLEISTERN

HANDLUNGSBEDARF

- Umsetzung der neuen Anforderungen bei allen **ZUKÜNFTIGEN DIENSTLEISTERN.**
- **BESTEHENDE AV-VERTRÄGE** sollten auf Anpassungsbedarf geprüft werden.
- **ZU ERWÄGEN**: Abschluss neuer, einheitlicher AV-Vereinbarungen mit allen Dienstleistern.

AUFTRAGSVERARBEITUNG

DATENSCHUTZKONFORME BEAUFTRAGUNG VON DIENSTLEISTERN

GENERELLES VORGEHEN

- **INVENTARISIERUNG** aller Dienstleister.
- **KATEGORISIERUNG** nach Auftragsverarbeitung, Funktionsübertragung und Weiteren.
- **ENTWURF EINES VERTRAGS** zur Auftragsverarbeitung.
- Ggf. **ENTWURF WEITERER VERTRÄGE**, bspw. zu Verschwiegenheitsverpflichtungen, Funktionsübertragungen und gemeinsamer Verarbeitung.
- **VEREINBARUNGEN** mit allen Dienstleistern (abhängig von der Kategorie).
- Gewährleistung angemessener **SCHUTZMAßNAHMEN.**

RISIKOMANAGEMENT IM DATENSCHUTZ

RISIKOMANAGEMENT IM DATENSCHUTZ

BEGRIFFLICHE KLÄRUNG

WER IST BETROFFEN?

- Risiken der "betroffenen Person" – natürliche Personen, deren Daten verarbeitet werden.
- Unternehmerische Risiken – der "Stelle", welche die Verarbeitung vornimmt.

Das Bußgeld-Risiko ist bspw. nach Auffassung einiger Aufsichtsbehörden kein Risiko, welches im datenschutzrechtlichen Sinne zu betrachten wäre, sondern ein unternehmerisches Risiko.

RISIKOMANAGEMENT IM DATENSCHUTZ

RISIKEN DER BETROFFENEN PERSON

- "**VERLUST DER KONTROLLE**" über personenbezogenen Daten
  - Unerlaubte Veröffentlichung / Offenbarung im Internet
  - Versand von E-Mails an unberechtigte Adressaten
  - Verlust der Verfügbarkeit von personenbezogenen Daten
- **VERLUST DER VERTRAULICHKEIT** von dem Berufsgeheimnis unterliegenden Daten

- **IDENTITÄTSDIEBSTAHL** oder **-BETRUG**
- **FINANZIELLE VERLUSTE**
- Andere erhebliche **WIRTSCHAFTLICHE ODER GESELLSCHAFTLICHE NACHTEILE**
- Unbefugte **AUFHEBUNG EINER PSEUDONYMISIERUNG**

- **EINSCHRÄNKUNG DER RECHTE** einer natürlichen Person
- Diskriminierung
- Rufschädigung

RISIKOMANAGEMENT IM DATENSCHUTZ

UNTERNEHMERISCHE RISIKEN

AUFSICHTSBEHÖRDEN

- Verhängung von **BUßGELDERN**
- **ANORDNUNGEN**
- Faktisch: **MEHRAUFWAND** durch die Bearbeitung von Anfragen der Aufsichtsbehörden

RECHTLICHE RISIKEN

- **SCHADENERSATZANSPRÜCHE** (materiell / immateriell)
- **VERBANDSKLAGERECHT**: U.a. Schadensersatzansprüche, Löschansprüche und Auskunftsansprüche können zukünftig durch Verbraucherverbände eingeklagt werden. Mittelbar wird dies Unternehmen zur Einhaltung ihrer datenschutzrechtlichen Verpflichtungen anhalten, da verstärkt mit Verbandsklagen zu rechnen ist.

RISIKOMANAGEMENT IM DATENSCHUTZ

UNTERNEHMERISCHE RISIKEN

REPUTATION

- Reputationsverlust durch das Bekanntwerden von Verstößen, Datenpannen oder generell als "unredlich" erachtetem Verhalten u.a. über
  - Tagespresse, Nachrichten
  - Webportale, neue Medien, virale Verbreitung

WIRTSCHAFTLICHE RISIKEN

- Verlust von **AUFTRAGGEBERN**, wenn deren Compliance-Richtlinien nicht eingehalten werden.
- Erstarken der **MARKTPOSITION** von **WETTBEWERBERN** in datenschutzsensitiven Branchen.
- Ausfall der IT bedingt **NICHTVERFÜGBARKEIT** von IT-Systemen und IT-Diensten. Mögliche Auswirkungen können **ERTRAGSAUSFALL** und **VERTRAGSSTRAFEN** sein.

RISIKOMANAGEMENT IM DATENSCHUTZ

UNTERNEHMERISCHE RISIKEN AUßERHALB DES DATENSCHUTZES

GESCHÄFTS- UND BETRIEBSGEHEIMNISSE

- Vertraulichkeit: Industriespionage / Datendiebstahl.
- Verfügbarkeit: Fehlerhafte Datensicherung.
- Integrität: Manipulation.

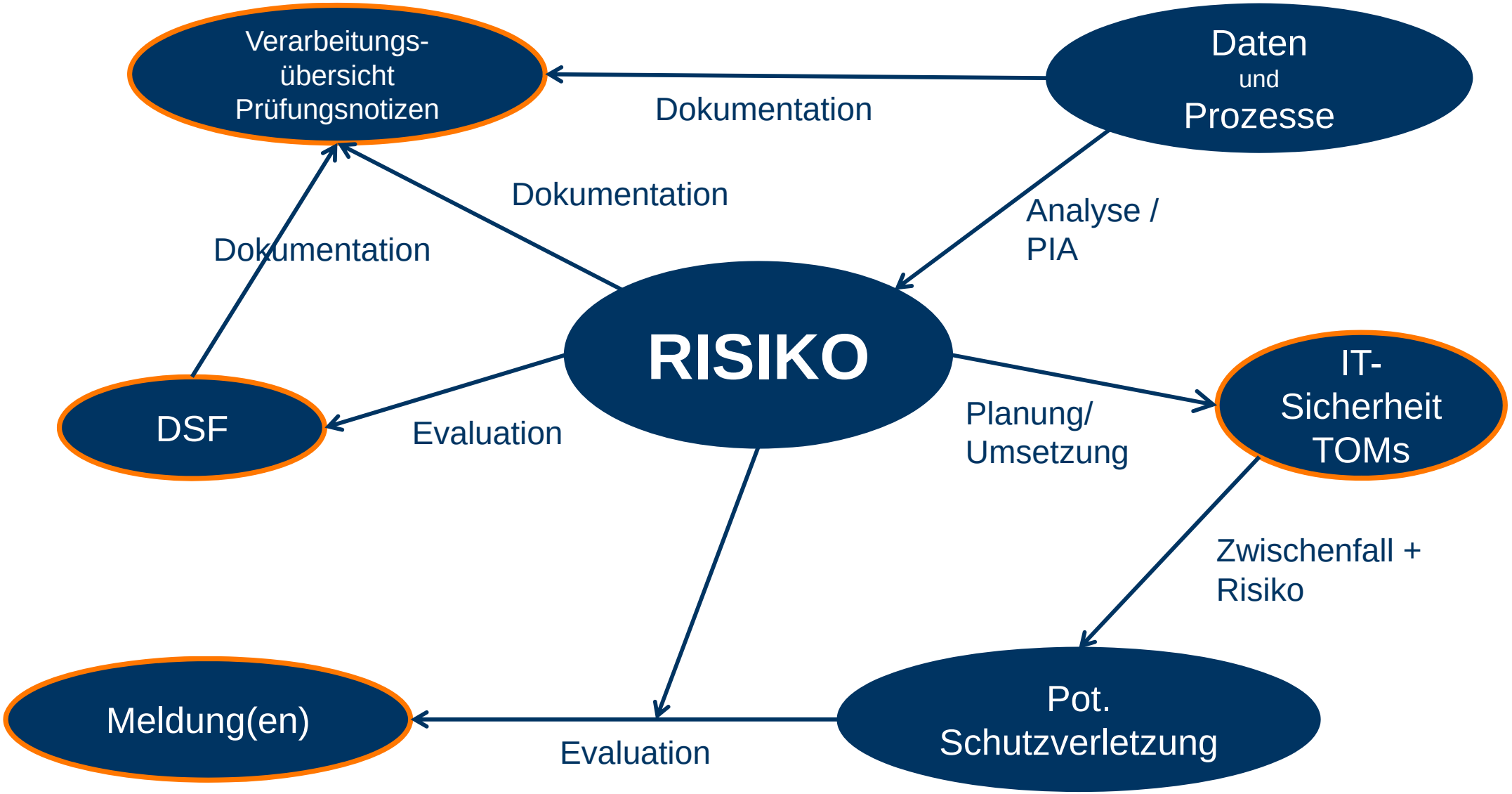
VERFÜGBARKEIT VON ZENTRALEN DIENSTEN UND IT-SYSTEMEN

Einschränkung durch:

- DDOS-Attacken.
- Bauarbeiten, Ausfall eines Dienstleisters.
- Ansturm bei Rabatt-Aktionen und besonderen Anlässen, bspw. Black Friday, Weihnachten.
- Verschleiß von IT-Komponenten, Wartungsfehler.

RISIKOMANAGEMENT IM DATENSCHUTZ

RISIKO IN DER DSGVO



IT-SICHERHEIT – INFORMATIONSSICHERHEIT

Der Blick über den Tellerrand

IT- UND INFORMATIONSSICHERHEIT

DER FEINE UNTERSCHIED – DATENSCHUTZ VS. IT- VS. INFORMATIONSSICHERHEIT

GEMEINSAMES ZIEL

Schutz von Werten und Gegenständen, die in der Obhut des Unternehmens liegen:

- Informationen
  - Geschäfts- und Betriebsgeheimnisse
  - Personenbezogene Daten
- Gegenstände (IT-Systeme, Software, andere Unternehmenswerte)
- Vermögen

FAZIT

Eine ganzheitliche Sicht auf Datenschutz sowie IT- und Informationssicherheit schafft Synergieeffekte und spart Ressourcen.

IT- UND INFORMATIONSSICHERHEIT

ANFORDERUNGEN AN DIE KONZEPTION ZU TREFFENDER MAßNAHMEN

BERÜCKSICHTIGUNG VON:

- **STAND DER TECHNIK** (Anpassung werden durch Zeitablauf erforderlich, auch wenn die Verfahren unverändert bleiben).
- Kosten der **IMPLEMENTIERUNG.**
- **ART UND UMFANG** der Datenverarbeitung.
- **ZWECKE** der Verarbeitung.
- **RISIKOBEURTEILUNG** nach Eintrittswahrscheinlichkeit und Schadenshöhe.

ANFORDERUNGEN AN DIE ÜBERWACHUNG DER MAßNAHMEN

- Einrichtung eines **KONTROLLVERFAHRENS** zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen Schutzmaßnahmen.
- Systematische Gewährleistung der **SICHERHEIT DER VERARBEITUNG.**
- **NACHVOLLZIEHBARKEIT**
  - des Verfahrens selbst
  - der operativen Umsetzung von Kontrollen

AUSBLICK

VORBEREITUNG AUF DEN 25. MAI 2018

- **PLANUNG** und **PRIORISIERUNG** der Anforderungen aus DSGVO, BDSG-neu und ggf. weiteren Gesetzen.
- **FRISTGERECHTE UMSETZUNG** der Tätigkeiten.

…DER BLICK IN DIE KRISTALLKUGEL

- Mit dem 25.Mai 2018 **beginnt** das Gelten der DSGVO erst.
- **AKTIONEN** von Aufsichtsbehörden?
- **REAKTIONEN** von Unternehmen?
- Das nächste Datenschutz-Gesetz ist schon in Sicht: Ende des Jahres kommt die **E-PRIVACY-VERORDNUNG.**

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

FIDES
Wir sind Vertrauen.

Wirtschaftsprüfer | Steuerberater
IT-Berater | Unternehmerberater

DIREKTWERBUNG IM EUROPÄISCHEN DATENSCHUTZRECHT

AUSWIRKUNGEN DER EU-DATENSCHUTZGRUNDVERORDNUNG UND DER E-PRIVACY-VERORDNUNG

DR. RALF KOLLMANN

Düsseldorf, 20.02.2018

Praxity
MEMBER
GLOBAL ALLIANCE OF INDEPENDENT FIRMS

INHALT

ÜBERBLICK ZUR RECHTSLAGE

ÜBERBLICK ZUR RECHTSLAGE

ZUKÜNFTIGE DATENSCHUTZRECHTLICHE REGELUNG VON DIREKTWERBUNG

POSTALISCHE WERBUNG

- Datenschutz-Grundverordnung (DSGVO)
- BDSG neu

ELEKTRONISCHE WERBUNG

- E-Privacy-Verordnung (EPVO)
- DSGVO
- BDSG neu

ÜBERBLICK ZUR RECHTSLAGE

DER BLICK IN DIE KRISTALLKUGEL

ANSPRUCH…

- Durch den Gesetzgeber **GEPLANT** war das Inkrafttreten der E-Privacy-Verordnung parallel zur EU-Datenschutzgrundverordnung am **25. MAI 2018**.
- Damit sollten durch die DSGVO ungeregelte Bereiche, insbesondere Online-Dienste sowie die Direktwerbung **RECHTZEITIG ZUM INKRAFTTRETEN** auf europäischer Ebene geregelt werden.

…UND WIRKLICHKEIT

- Eine Einigung zur Verabschiedung der EPVO ist den Beteiligten **NICHT RECHTZEITIG GELUNGEN**.
- Gegenwärtig wird von einem voraussichtlichen Inkrafttreten der EPVO **ANFANG 2019** ausgegangen.

DIE E-PRIVACY-VERORDNUNG (EPVO)

ÜBERBLICK

ENTWURFSSTATUS

- Die EPVO liegt gegenwärtig als **ENTWURF** vor – sie ist noch nicht verabschiedet.
- Es können sich folglich noch **ÄNDERUNGEN** ergeben.

UNEINIGKEITEN

- Es bestehen gegenwärtig Uneinigkeiten bei der Konkretisierung, bspw. zu
  - Umgang mit **COOKIES** (Cookie-Banner)
  - Erweiterung von Schutzmaßnahmen gegen **TRACKING**, einschließlich etwaig erforderlicher Einwilligungen
  - (Ggf. erweiterten/verpflichtenden) Vorschriften zur **VERSCHLÜSSELUNG** elektronischer Kommunikation.

DIE E-PRIVACY-VERORDNUNG (EPVO)

ÜBERBLICK

- Die geplante **E-PRIVACY-VERORDNUNG** soll die bisher geltende EU-Richtlinie 2002/58/EG (E-Privacy-Richtlinie) ersetzen.
- Sie wird die **DSGVO** in Bereichen der elektronischen Kommunikation und Spezialregelungen der Werbung ergänzen bzw. präzisieren.
- Die EPVO novelliert (verdrängt) damit – **voraussichtlich** – Vorschriften aus TMG, TKG und UWG.
- Die nicht novellierten Regelungen der novellierten Gesetze haben **WEITERHIN BESTAND**.
- Als EU-Verordnung wird sie – ebenso wie die DSGVO – **UNMITTELBAR UND VORRANGIG** in allen EU-Ländern geltendes Recht und bedarf nicht einer Umsetzung in nationale Rechtsnormen.

DIE E-PRIVACY-VERORDNUNG (EPVO)

ZIELGRUPPEN

PRIMÄRE ZIELGRUPPEN DER EPVO

- Telekommunikationsdienste-Anbieter
- Softwareentwickler im Telemedien- und Telekommunikationsbereich
- Telemediendienste-Anbieter
- Online Content-Provider
- Anbieter von Over-the-Top-Diensten
- Betreiber von Direktwerbung

FOKUS HEUTE: REGELUNGEN ZUR DIREKTWERBUNG

WAS BEDEUTET DIREKTWERBUNG?

DIREKTWERBUNG

BEGRIFFSBESTIMMUNG

DIREKTWERBUNG (ART. 4 ABS. 3 LIT. F EPVO)

- schriftlich oder mündlich
- an einen oder mehrere bestimmte oder bestimmbare Endnutzer elektronischer Kommunikationsdienste gerichtet
- auch mittels automatischer Anruf- und Kommunikationssysteme
- mit oder ohne menschliche Beteiligung, mittels E-Mail, SMS-Nachrichten usw.
- umfasst auch telefonische Werbung

POSTALISCHE WERBUNG

DIREKTWERBUNG

B2B ODER B2C?

Es existieren in der DSGVO **KEINE UNTERSCHIEDLICHEN REGELUNGEN** für die Adressierung von Privat- oder Geschäftskunden.

ALTES RECHT

- **POST**: Analog B2C (bspw. Listenprivileg, Hinweis auf Widerspruchsrecht und Herkunft der Daten etc.)
- **TELEFON**: Mutmaßliche Einwilligung bei B2B zu prüfen (§ 7 Abs. 2 Nr. 2 UWG)
- **E-MAIL**: Bestandskundenregelung (Bestandskunden, Transparenz, kein Widerspruch)

NEUES RECHT

- **POST**: Analog B2C (bspw. per Interessenabwägung)
- Interessenabwägung kann im B2B-Fall eher zu einer positiven Einschätzung gelangen als bei B2C
- **TELEFON**: Öffnungsklausel zur Wahrung berechtigter Interessen (Art. 16 Abs. 5),
  - ggf. + mutmaßliche Einwilligung
  - **E-MAIL**: Neue Bestandkundenregelung (16 Abs. 2 EPVO) entspricht grundsätzlich § 7 Abs. 3 UWG, alternativ Einwilligung

POSTALISCHE WERBUNG

RECHTSGRUNDLAGEN

- Die DSGVO beinhaltet **KEINE EXPLIZITE ERLAUBNISNORM** für Werbung.
- Die Verarbeitung aufgrund des **LISTENPRIVILEGS** des BDSG a.F. **ENTFÄLLT**.
- Es existieren in der DSGVO keine unterschiedlichen Regelungen für die Adressierung von Privat- oder Geschäftskunden.
- Werbung darf und muss zukünftig auf **GENERISCHE ERLAUBNISNORMEN** gestützt werden.

ZULÄSSIGKEITSGRUNDLAGEN

- Interessenabwägung
- Einwilligung
- Zweckänderung

POSTALISCHE WERBUNG

INTERESSENABWÄGUNG

- Verarbeitung personenbezogener Daten auf Grundlage berechtigter Interessen des Verantwortlichen.
- Die schutzwürdigen Belange der Betroffenen dürfen nicht überwiegen.
- Eine **INTERESSENABWÄGUNG IST DURCHZUFÜHREN** und zu dokumentieren.
- Die Argumentation wird durch die Erwägungsgründe erleichtert:

"DIREKTWERBUNG KANN EIN BERECHTIGTES INTERESSE DARSTELLEN." (EG 47)

POSTALISCHE WERBUNG

INTERESSENABWÄGUNG

MAßNAHMEN ZUR POSITIVEN GESTALTUNG EINER INTERESSENABWÄGUNG:

- **VERMEIDUNG** von besonders **UMFANGREICHEN** oder **SENSIBLEN** Daten (die Nutzung von "besonderen Daten" ist grundsätzlich ausgeschlossen).
- Vermeidung von umfassenden, automatisierten **SELEKTIONSVERFAHREN**, inkl. Profiling und Scoring.
- **AGGREGATION** von Selektionskriterien bzw. selektierten Werten.
- Treffen von technischen und organisatorischen **SCHUTZMAßNAHMEN.**

B2B

- **FOKUSSIERUNG** der Selektionskriterien auf Informationen über das **UNTERNEHMEN** selbst (nicht Einzelpersonen wie Ansprechpartner), bspw. Branche, Tätigkeitsbereiche, Umsatz
- **VERMEIDUNG** von Daten aus dem **PERSÖNLICHEN UMFELD** der Adressaten

POSTALISCHE WERBUNG

EINWILLIGUNG

- Werbung kann – wie jede Verarbeitung personenbezogener Daten – auf die **EINWILLIGUNG** der Betroffenen gestützt werden.
- Aufgrund des potentiell großen damit verbundenen **AUFWANDS** wird die Einwilligung bei der Werbung voraussichtlich nachrangig eingesetzt werden, bspw. wenn die Zugrundelegung einer anderen Rechtsgrundlage nicht möglich ist.
- **BESTEHENDE EINWILLIGUNGEN GELTEN WEITERHIN**, wenn sie der Art nach den Bedingungen der DSGVO entsprechen (EG 171 S. 3).

POSTALISCHE WERBUNG

ZWECKÄNDERUNG

VORAUSSETZUNGEN

- Die (personenbezogenen) Daten wurden ursprünglich nicht zu Zwecken der Werbung erhoben.
- Die Zwecke der ursprünglichen Datenerhebung müssen jedoch mit Werbezwecken vereinbar sein (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO).
- Die **GRENZEN DER WEITERVERARBEITBARKEIT** (EG 50) sind weit ausgelegt, sollten jedoch geprüft werden.
- Eine **DOKUMENTATION** der Zwecke und eine Herleitung der Vereinbarkeit ist erforderlich, bspw. in der Verarbeitungsübersicht.

Da im kommerziellen Umfeld Daten regelmäßig auch zu Werbezwecken erhoben werden (und darauf hingewiesen wird), ist der Rechtsgrundlage der **INTERESSENABWÄGUNG** i.d.R. der Vorzug zu geben.

POSTALISCHE WERBUNG

WAS KANN AUßERDEM WICHTIG SEIN?

AUFTRAGSVERARBEITUNG

Wurde ein AV-Dienstleister beauftragt?

AUTOMATISIERTE SELEKTIONSVERFAHREN / PROFILING

Werden automatisierte Verfahren zur Ermittlung der Adressaten eingesetzt?

PSEUDONYMISIERUNG (BSPW. BEI WEB-BASIERTER WERBUNG)

Umsetzung individueller Customer-Experience in der Web-Präsenz mittels Pseudonymisierung?

GRUNDSÄTZLICHE ANFORDERUNGEN AN DEN DATENSCHUTZ

- Angemessene technische und organisatorische Maßnahmen
- Datenschutz-Management
- IT-Sicherheits-Management

ELEKTRONISCHE WERBUNG

ELEKTRONISCHE WERBUNG: E-MAIL

RECHTSGRUNDLAGEN ZUR WERBUNG PER E-MAIL

Die DSGVO beinhaltet **KEINE EXPLIZITE ERLAUBNISNORM** für Werbung.

Es verbleiben als **ALTERNATIVEN** zur Umsetzung:

- Einwilligungsbasierte Werbung
- Bestandskundenregelung (EPVO / UWG)

ELEKTRONISCHE WERBUNG: E-MAIL

EINWILLIGUNG

- Werbung per E-Mail (an natürliche Personen) ist grundsätzlich nach **EINWILLIGUNG** zulässig (Art. 16 Abs. 1 EPVO)
- Die **ANFORDERUNGEN** an die Einwilligung sind **UMFASSEND** und **AUFWÄNDIG** in der Umsetzung und Verwaltung (Art. 9 EPVO – Verweis auf Art. 7 DSGVO)
- **NACHWEISBARKEIT** der Einwilligung erforderlich

ELEKTRONISCHE WERBUNG: E-MAIL

BESTANDSKUNDEN

VORAUSSETZUNGEN

- Die E-Mail-Adresse des Kunden wurde im Zusammenhang mit dem Verkauf eines **EIGENEN PRODUKTS ODER EINER DIENSTLEISTUNG** erhalten
- Verarbeitung im Einklang mit der DSGVO
- **WERBUNG FÜR EIGENE ÄHNLICHE PRODUKTE** oder Dienstleistungen
- Informierung über und Berücksichtigung von **WERBEWIDERSPRÜCHEN**
- Berücksichtigung des **KOPPLUNGSVERBOTS**

B2B – GRUNDSÄTZLICH ANALOG ZU B2C

- Einwilligung
- Bestandkundenwerbung

ELEKTRONISCHE WERBUNG: TELEFONWERBUNG

RECHTSGRUNDLAGEN

- Bei Telefonwerbung muss die **EINWILLIGUNG** des Adressaten vorliegen.
- Eine **EXPLIZITE ERLAUBNISNORM** analog zur Bestandskundenwerbung per E-Mail **EXISTIERT NICHT**.

- Ausweitung des **VERBOTS DER RUFNUMMERNUNTERDRÜCKUNG**
  - Nennung der Rufnummer oder
  - eines "Codes, der deutlich macht, dass es sich um einen Werbeanruf handelt"
  - Durchführungsmaßnahmen hierzu werden durch die EU-Kommission veranlasst

- Es besteht eine **ÖFFNUNGSKLAUSEL** zur **ERWEITERUNG DER ZULÄSSIGKEIT** auf alle Personen, die nicht widersprochen haben.
- Zu deren Umsetzung muss das Inkrafttreten der EPVO abgewartet werden.

ELEKTRONISCHE WERBUNG: TELEFONWERBUNG

B2B

- **ÖFFNUNGSGEBOT**: Verpflichtung der nationalen Gesetzgeber zur Wahrung der Interessen juristischer Personen bei elektronischer Direktwerbung (Art. 16 Abs. 5)
- Die **ÖFFNUNGSKLAUSEL** zur **ERWEITERUNG DER ZULÄSSIGKEIT** auf alle Personen, die nicht widersprochen haben, könnte auch im B2B-Bereich gelten. Dies bleibt abzuwarten.
- **BESTEHENDE REGELUNG**: Ggf. Stützung auf die **MUTMAßLICHE EINWILLIGUNG** (§ 7 Abs. 2 Nr. 2 UWG) erforderlich, solange keine Novellierung auf nationaler Ebene erfolgt.

RECHTE UND INFORMATIONSPFLICHTEN

ZUSAMMENFASSUNG

ALLGEMEINE INFORMATIONSPFLICHT (DSGVO)

UMFASSENDE INFORMIERUNG der betroffenen Person:

- bei direkter Datenerhebung
- bei indirekter Datenerhebung

EINWILLIGUNG

INFORMATIONSPFLICHT über das **WIDERRUFSRECHT** der erteilten Einwilligung.

WIDERSPRUCHSRECHT GEGEN DIREKTWERBUNG

- Berücksichtigung von Widersprüchen und Informationspflicht
  - bei der **DATENERHEBUNG** und
  - bei jeder **ANSPRACHE**
  - Kostenlose und "einfache" Möglichkeit des **WIDERSPRUCH**s
- Das Widerspruchsrecht gilt auch bei jeder Verarbeitung aufgrund eines **BERECHTIGTEN INTERESSES**.

RECHTE UND INFORMATIONSPFLICHTEN

ZWECKÄNDERUNG

Zusätzliche Informationspflicht bei Verarbeitung aufgrund von Zweckänderung.

WERBUNG ÜBER "ELEKTRONISCHE KOMMUNIKATIONSDIENSTE"

Zusätzliche Informationspflicht von Endnutzern über:

- den **WERBECHARAKTER** der Nachricht und
- die **IDENTITÄT** des Veranlassers, in dessen Namen die Nachricht übermittelt wird
- Bereitstellung von **INFORMATIONEN ZUM WIDERRUF,** um die Einwilligung in den weiteren Empfang von Werbenachrichten widerrufen zu können (bspw. Kontaktdaten).

AUSBLICK

ALLES BEIM ALTEN?

- Für deutsche Unternehmen gibt es bei der Direktwerbung per E-Mail und Telefon **KAUM ÄNDERUNGEN** gegenüber den bisherigen Regelungen des UWG (bzw. BDSG).
- Wer sich jetzt bereits an die geltenden Regelungen hält und keine Änderungen plant, hat in diesem Bereich voraussichtlich **WENIG HANDLUNGSBEDARF.**
- Insbesondere ist davon auszugehen, dass die EPVO keine Regelungen zur postalischen Werbung trifft.

DIE EPVO IST NOCH NICHT VERABSCHIEDET

- Die dargelegte Sicht basiert auf dem bestehenden Entwurf der EPVO. **ÄNDERUNGEN SIND WAHRSCHEINLICH.**
- Auch in der EPVO sind **ÖFFNUNGSKLAUSELN** vorgesehen. Änderungen sind damit nicht nur auf **EUROPÄISCHER EBENE**, sondern auch auf **NATIONALER EBENE** möglich.

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

Nölle & Stoevesandt

Rechtsanwälte

Die Auftragsverarbeitung nach der DSGVO

DR. STEFANIE KLEINMANNS

DÜSSELDORF, 20. FEBRUAR 2018

Nölle & Stoevesandt

1. Einleitung
2. Auftrags(daten)verarbeitung nach altem Recht
3. Auftragsverarbeitung in der DSGVO
4. Auftragsverarbeitung im Konzern
5. Haftung
6. Ausblick

1. EINLEITUNG.

WORUM GEHT ES?

Einbindung Dritter in die Verarbeitung personenbezogener Daten.

Werden personenbezogene Daten ausschließlich weisungsgebunden **im Auftrag durch andere Stellen** erhoben, verarbeitet oder genutzt, ist dies eine Auftragsverarbeitung. Eine klassische **Auftragsverarbeitung** findet statt in den Bereichen:

- Externe Lohn- und Gehaltsabrechnungen,
- Versendung von Briefen über sog. Letter Shops,
- Wartung von IT-Anlagen,
- Cloud Computing
- etc.

Abzugrenzen ist die Auftragsverarbeitung von der **Funktionsübertragung**, bei der durch den Verantwortlichen neben der Verarbeitung auch die **zugrunde liegende Aufgabe** an einen Dienstleister übertragen wird.

1. EINLEITUNG.

Mit dem **Inkrafttreten** der europäischen Datenschutz-Grundverordnung (DS-GVO) am 24. Mai 2016 und deren **Wirksamwerden am 25. Mai 2018** gelten ab diesem Datum auch hinsichtlich der Auftragsverarbeitung (AV) die Regelungen der **DSGVO unmittelbar** in Deutschland.

Diese **lösen** die nationalen Regelungen für die Datenverarbeitung im Auftrag **ab**.

1. EINLEITUNG.

Die **Anforderungen** an die datenschutzrechtlichen Inhalte von **Auftragsverarbeitungs-Verträgen** wurden in der DSGVO festgelegt.

ACHTUNG:

- Es gibt **Abweichungen** zur bisherigen Rechtslage.
- Die Regelungen der DSGVO gelten **nicht nur** für **zukünftige** Vertragsabschlüsse, sondern auch für alle **schon vorhandenen** und **noch laufenden** Verträge **ab Wirksamwerden der DSGVO**.
- Im Falle von **Verstößen** drohen **hohe Bußgelder**.

2. AUFTRAGS(DATEN)VERARBEITUNG NACH ALTEM RECHT.

Derjenige, der im Einklang mit § 11 BDSG **für den** und **unter Kontrolle** des Verantwortlichen Daten erhebt, verarbeitet oder nutzt, wird **nicht** als **Dritter**, sondern als **organisatorischer Teil** des Verantwortlichen behandelt **(Sonderrolle der Auftragsverarbeitung**).

VORAUSSETZUNGEN:

- Auftragsverarbeiter führt **strikt** nach den **Weisungen** des Auftraggebers vorgegebene Tätigkeiten in Bezug auf die personenbezogenen Daten aus.
- Es wird eine Vereinbarung entsprechend den **inhaltlichen Vorgaben des § 11 BDSG** geschlossen.
- Die Verarbeitung erfolgt **in einem Mitgliedstaat der EU** oder **des EWR**.
- Die Vereinbarung genügt der **Schriftform**.

2. AUFTRAGS(DATEN)VERARBEITUNG NACH ALTEM RECHT.

FOLGE:

- **Privilegierung** der Auftragsverarbeitung,
- Umfasst sind auch **besondere Datenkategorien** (§ 3 Abs. 9 BDSG),
- **Verantwortlich** für die Rechtmäßigkeit der Auftragsverarbeitung ist **allein der Auftraggeber.**

3. AUFTRAGSVERARBEITUNG IN DER DSGVO.

„Auftragsdatenverarbeitung“ → **„Auftragsverarbeitung“**

NEU:

Der Auftragsverarbeiter ist **nicht mehr Teil** des Verantwortlichen, sondern eine von ihm grundsätzlich **unabhängige Person** als Empfänger personenbezogener Daten i.S.v. Art. 4 Nr. 9 DSGVO.

ABER:

Es bleibt bei der Privilegierung. Es müssen ausschließlich die formalen und inhaltlichen **Anforderungen** des **Art. 28 DSGVO** eingehalten werden.

3. AUFTRAGSVERARBEITUNG IN DER DSGVO.

AUSWAHL DES AUFTRAGSVERARBEITERS, WEITERE AUFTRAGSVERARBEITER .

Der Auftraggeber **darf nur** Auftragsverarbeiter heranziehen, die hinreichende Garantien dafür bieten, dass

- **geeignete technische und organisatorische Maßnahmen** getroffen werden und
- der **Schutz** der Rechte der betroffenen Personen **gewährleistet** ist.

Bei der Beauftragung von Unterauftragnehmern **muss** festgelegt werden (Art. 28 Abs. 3 S. 2 lit. d i.V.m. Art. 28 Abs. 2 DSGVO):

- **Zustimmungsvorbehalt** des Auftraggebers bei Beauftragung weiterer Auftragsverarbeiter,
- **Widerspruchsmöglichkeit** bei vorheriger allgemeiner Genehmigung zur Beauftragung weiterer Auftragsverarbeiter, **oder**
- **Verbot** von weiteren Auftragsverarbeitern.

3. AUFTRAGSVERARBEITUNG IN DER DSGVO.

INHALTLICHE ANFORDERUNGEN AN DEN VERTRAG ODER ANDERES RECHTSINSTRUMENT.

Die Verarbeitung hat auf der **Grundlage eines Vertrages** oder eines anderen Rechtsinstruments zu erfolgen. **Darin sind festzulegen**:

- Gegenstand und Dauer des Auftrags,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten,
- Kategorien betroffener Personen,
- Pflichten und Rechte des Auftraggebers,
- Mindestinhalt der Pflichten des Auftragnehmers (Art. 28 Abs. 3 S. 2).

3. AUFTRAGSVERARBEITUNG IN DER DSGVO.

MINDESTINHALT DER PFLICHTEN DES AUFTRAGSVERARBEITERS, ART. 28 ABS. 3 S. 2 DSGVO.

- Pflicht zur Verarbeitung **nur auf dokumentierte Weisung** des Verantwortlichen, auch in Bezug auf die Übermittlung an ein Drittland.
- Verpflichtung der zur Verarbeitung der Daten befugten Personen auf **Vertraulichkeit.**
- Pflicht, alle gem. Art. 31 DSGVO erforderlichen **Maßnahmen zur Sicherheit** der Datenverarbeitung zu ergreifen.
- Pflicht, die Vorgaben für die Beauftragung von **Unterauftragnehmern** einzuhalten.
- Pflicht, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen **zu unterstützen**.
- Pflicht, den Auftraggeber bei der **Meldung** von Datenschutzverletzungen, **Datenschutz-Folgeabschätzungen** und vorherigen **Konsultationen** durch Aufsichtsbehörden zu unterstützen.
- Pflicht zur **Löschung** oder **Rückgabe** nach Abschluss der Erbringung der Verarbeitungsleistungen.
- Pflicht zur Zurverfügungstellung **aller erforderlichen Informationen** zum Nachweis der Einhaltung der niedergelegten Pflichten und Ermöglichen von Überprüfungen.

3. AUFTRAGSVERARBEITUNG IN DER DSGVO

ELEKTRONISCHES FORMAT.

Der Vertrag oder ein anderes Rechtsinstrument sind **schriftlich** abzufassen, gemeint ist bloße **Textform**, nicht die enge Schriftform des § 126 BGB (eigenhändige Unterschrift).

WEITERE PFLICHTEN DES AUFTRAGSVERARBEITERS.

- Ggf. Pflicht zur **Führung eines Verzeichnisses** über Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- **Meldepflicht** bei einer Verletzung des Schutzes personenbezogener Daten, die ihm bekannt wird.
- Pflicht zur **Bestellung eines Vertreters** in der Union, Art. 27 DSGVO.
- Pflicht zur **Zusammenarbeit** mit der Datenschutz-Aufsichtsbehörde, Art. 31 DSGVO.
- Ggf. Pflicht zur Bestellung eines **Datenschutzbeauftragten**, Art. 37 DSGVO.

3. AUFTRAGSVERARBEITUNG IN DER DSGVO.

AUFTRAGSVERARBEITUNG IM AUSLAND.

ALTE RECHTSLAGE:

Privilegierungswirkung war **beschränkt** auf Auftragsverarbeitung in der EU oder im EWR.

NEUE RECHTSLAGE:

Keine räumliche Begrenzung der Privilegierungswirkung.

Aber: Die Prüfung nach Art. 44 ff. DSGVO, **ob** personenbezogene Daten in einen **Drittstaat** übertragen werden dürfen, bleibt davon unberührt und ist weiterhin zusätzlich erforderlich.

4. AUFTRAGSVERARBEITUNG IM KONZERN.

GRUNDSATZ.

Es gibt auch nach der DSGVO **kein Konzernprivileg**, d.h. jede zu einem Konzern / einer Unternehmensgruppe gehörende Gesellschaft ist als eigenständiges Objekt zu behandeln.

Aber: „**kleines Konzernprivileg**“ in ErwG 48 DSGVO

Danach sind Interessen von Konzernen in der **Interessenabwägung** zu prüfen, bereits bislang berücksichtigte Interessen fließen weiterhin in die Abwägungen mit ein.

Im Falle der **Ausübung eines Widerspruchsrechts** des Betroffenen nach Art. 21 Abs. 1 DSGVO kann das „kleine Konzernprivileg“ des ErwG 48 DSGVO zwar in die Interessenabwägung fließen, aber **nicht pauschal** dazu führen, dass das Konzerninteresse den Widerspruch des Betroffenen überwiegen würde.

4. AUFTRAGSVERARBEITUNG IM KONZERN.

KONZERNBEZUG IN WEITEREN REGELUNGEN.

ONE-STOP-SHOP BEI KONTROLLE DURCH DIE AUFSICHTSBEHÖRDEN.

Bei der **Überwachung der Datenschutzgesetze** durch die Aufsichtsbehörden wird ein **Kooperations- und Kohärenzverfahren** eingeführt, alle Aufsichtsbehörden sind zwar beteiligt, allerdings wird nach Art. 56 Abs. 1 DSGVO eine **federführende Aufsichtsbehörde am Sitz der Hauptniederlassung** eines Verantwortlichen bestimmt.

KONZERNDATENSCHUTZBEAUFTRAGTER.

Künftig kann **ein Datenschutzbeauftragter für mehrere Konzernunternehmen** als interner Datenschutzbeauftragter bestellt werden, gem. Art. 37 Abs. 2 DSGVO kann eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen, sofern seine Erreichbarkeit sichergestellt ist.

BERECHNUNG DER BUßGELDER.

Für die Berechnung der Bußgelder ist nach Art. 83 Abs. 4 und 5 DSGVO wohl auf den **weltweit erzielten Umsatz** des jeweiligen **Einzelunternehmens** abzustellen und nicht auf den **Konzernumsatz** (umstritten).

Nölle & Stoevesandt

4. AUFTRAGSVERARBEITUNG IM KONZERN.

SONDERFALL WARTUNGSVERTRÄGE.

Bisher bestand bei der Tätigkeit von Wartungs- oder Serviceunternehmen, die im Rahmen ihrer Betreuungs- und Reparaturtätigkeit personenbezogene Daten zur Kenntnis nehmen konnten gem. § 11 Abs. 5 BDSG die **Pflicht**, **Auftragsdatenverarbeitungs-verträge abzuschließen** (Online-Überwachung von Datenverarbeitungsanlagen, Fernwartung).

NEUE RECHTSLAGE.

In der **DSGVO** ist eine vergleichbare Regelung **nicht enthalten**. Soweit im Rahmen der Wartung ein **Zugriff** auf personenbezogene Daten **nicht Teil** des Vertrages ist, jedoch **nicht ausgeschlossen** werden kann (z.B. im Rahmen technischer Kontrollen), ist **kein Abschluss** eines Auftragsverarbeitungsvertrages notwendig. Eine **Verschwiegenheits-erklärung** reicht in solchen Fällen aus.

5. HAFTUNG.

Derzeit haftet gem. § 7 BDSG **ausschließlich die verantwortliche Stelle** gegenüber den Betroffenen aus der Verletzung von Datenschutzrechten. Bei der Auftragsdaten-verarbeitung ist bisher stets nur der Auftraggeber „verantwortliche Stelle“. Eine Haftung des Auftragsverarbeiters kommt **nur** in **Ausnahmefällen** in Betracht.

NACH NEUER RECHTSLAGE.

- haften **Auftraggeber und Auftragsverarbeiter** unmittelbar gegenüber dem Geschädigten **gesamtschuldnerisch**, aber Exkulpationsmöglichkeit des Auftragsverarbeiters (Art. 82 Abs. 2 S. 2 DSGVO),
- umfasst die datenschutzrechtliche Haftung künftig gem. Art. 81 Abs. 1 DSGVO auch **immaterielle Schäden**,
- drohen im Falle von Verstößen **hohe Bußgelder** bis zu EUR 10.000.000 oder bis zu 2% des gesamten weltweit erzielten Vorjahresumsatzes des Unternehmens (Art. 83 Abs. 4 lit. a) DSGVO).

6. AUSBLICK.

- Nach jetzigem Stand wurde das Anforderungskonzept für die Einschaltung von Dienstleistern **weiter entwickelt**, **ohne** es zu **revolutionieren**.
- Zahlreiche vertraglich zu regelnde Pflichten ergeben sich künftig **unmittelbar aus dem Gesetz**.
- Für Konzerngesellschaften gibt es keine Änderungen, ein **Konzernprivileg** gibt es auch zukünftig **nicht**.
- Eine erhebliche **Haftungsverschärfung** ergibt sich aus der gemeinsamen Verantwortlichkeit von Auftragsverarbeiter und Auftraggeber, insbesondere für Auftragsverarbeiter.
- Die Höhe der **tatsächlich** verhängten **Bußgelder** bleibt abzuwarten.

Nölle & Stoevesandt

EIN GESPRÄCH BEWEGT MEHR. IHR ANSPRECHPARTNER.

DR. STEFANIE KLEINMANNS

POSITION	Rechtsanwältin
KONTAKTDATEN	Telefon: +49 (421) 3013-165 E-Mail: sk@noelle-stoevesandt.de
KURZVITA	• Jahrgang 1981 • Jurastudium in Rostock, Leuven/Belgien und Bremen • Referendariat in Bremen, 2 Staatsexamen 2009 • Promotion bei Prof. Dr. Ansgar Ohly, Bayreuth, 2013 • Rechtsanwältin seit 2010 • Seit Mai 2010 bei Nölle & Stoevesandt
QUALIFIKATION	• Rechtsanwältin
TÄTIGKEITSSCHWERPUNKTE/ RELEVANTE ERFAHRUNGEN	• Gesellschaftsrecht • Unternehmenstransaktionen • Vertragsrecht

Nölle & Stoevesandt

Rechtsanwälte

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