The project is co-funded by the REC Programme of the European Union

Training of Lawyers on the European Data Protection Reform

#TRADATA

HÄRTING

DSGVO (DATENSCHUTZ-GRUNDVERORDNUNG)

Niko Härting | haerting@haerting.de - Lasse Konrad | konrad@haerting.de

„Die Schlüsselanforderungen der neuen DSGVO in der Anwaltspraxis “

Betroffenenrechte

The project is co-funded by
the REC Programme
of the European Union

GRUNDLAGEN

- Im Grundsatz wie bisher:
  - Auskunftsrecht und Zugriffsrecht
  - Recht auf Berichtigung
  - Recht auf Löschung
  - Recht auf Einschränkung der Verarbeitung (Sperrung)
  - Aber im Detail zum Teil Ausweitung der Rechte (z.B. unverzügliche Beantwortung von Auskunftsansprüchen)
- Neu sind:
  - Widerspruchsrecht
  - Widerrufsrecht
  - Recht auf Vergessenwerden
  - Recht auf Datenübertragbarkeit (Datenportabilität)
- Insgesamt deutliche Stärkung der Betroffenenrechte!

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

ALLGEMEINE ANFORDERUNGEN ART. 12 DSGVO

- Allgemeine Anforderungen an die Betroffenenrechte gem. Art. 12 DSGVO
  - Erhöhte Transparenz, insbesondere bei Kindern
  - Erleichterung Rechtsausübung
  - Grundsätzlich unverzügliche Umsetzung
  - Keine Formvorschriften
  - Unentgeltlichkeit
  - Identitätsnachweis
  - Rechtsbehelfsbelehrung bei Ablehnung eines Ersuchens
- Hierauf gilt es sich vorzubereiten!

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

ALLGEMEINE ANFORDERUNGEN ART. 12 DSGVO

- Beantwortungspflicht
  - Information darüber welche Maßnahmen ergriffen worden sind
  - Betroffener muss nachvollziehen können, ob sein Antrag vollständig erfüllt oder abgelehnt wurde
  - Pflicht zur Rechtsbehelfsbelehrung bei Antragsablehnung
- Grundsätzlich unverzügliche Unterrichtung
  - Höchstfrist 1 Monat ab Antragseingang (nur in Ausnahmen)
  - Nur bei Beabsichtigung einer Positivantwort darf weitere 2 Monate verlängert werden (in schwierigen Fällen)
- Keine Formvorschrift für Geltendmachung und Erfüllung
- Unentgeltlichkeit (Ausnahme Missbrauch)
  - Offensichtlich unbegründete Anträge
  - Exzessive Anträge

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

ALLGEMEINE ANFORDERUNGEN ART. 12 DSGVO

- Identifizierung der Betroffenen Person
  - Identifizierung im Datenbestand nicht möglich
  - Zweifel an der Identität
  - Art. 11 DSGVO
    - Kann der Verantwortliche nachweisen, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, muss der Betroffene hierüber unterrichtet werden, sofern möglich
      - ➢ In diesen Fällen finden die Artikel 15 bis 20 DSGVO keine Anwendung
      - ➢ Betroffene Person kann zusätzliche Informationen bereitstellen, die eine Identifizierung ermöglichen

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

AUSKUNFTSRECHT ART. 15

- Formfreier Antrag
- Zu erteilende Auskünfte über:
  - Verarbeitungszwecke (ohne Rechtsgrundlage)
  - Datenkategorien
  - Empfängern / Empfängerkategorien
  - Speicherdauer oder Kriterien für die Festlegung der Speicherdauer
  - Betroffenenrechte (exkl. Auskunft)
  - Beschwerderecht
  - Datenquelle
  - Automatisierten Entscheidungsfindung / Profiling
  - Drittstaatentransfer
- Kopie der personenbezogene Daten

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

AUSKUNFTSRECHT ART. 15

- Verweis auf die Informationspflichten ist nicht ausreichend
- Auskunft erstreckt sich über die personenbezogenen Daten der betroffenen Person, die ihr Anspruch auf Auskunft geltend macht
- Bereitstellung einer Kopie, für jede weitere Kopie kann ein angemessenes Entgelt verlangt werden
  - Einschränkung im Falle einer Kollisionslage mit Rechten Dritter denkbar
- Zwingend: Prozess schaffen für Abarbeitung von Auskunftsansprüchen
- Empfehlung: Einrichtung eines Betroffenenrechte-Managements
- Fernzugang ermöglichen, wenn Implementierungskosten nicht unverhältnismäßig sind

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

AUSKUNFTSRECHT: AUSNAHMEN

- Im BDSG-neu wird von der Öffnungsklausel des Art. 23 DSGVO Gebrauch gemacht:

  „Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 … besteht … nicht, wenn … die Daten

  a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder

  b) ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen

  und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.“

RECHT AUF BERICHTIGUNG ART. 16

- Berichtigung „unrichtiger“ personenbezogener Daten (Art. 16 S. 1 DSGVO)
  - Pflicht des Verantwortlichen, allen Empfängern dieser Daten die Berichtigung mitzuteilen
  - Betroffenen steht ein ergänzendes Auskunftsrecht über die Empfänger zu
  - Daten müssen bis zur Berichtigung für die Verarbeitung gesperrt werden
  - Beschränkt sich auf Tatsachen, Werturteile (z.B. geschätzte Daten) sind ausgenommen
- Vervollständigung richtiger personenbezogener Daten (Art. 16 S. 2 DSGVO)
  - Beschränkt sich auf das Ergänzen eines richtigen Datums um weitere Informationen
  - Ziel ist ein zutreffenderer Aussagegehalt
  - Die Verarbeitung zusätzlicher Informationen ist auf den ursprünglichen Verarbeitungszweck beschränkt

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

RECHT AUF LÖSCHUNG ART. 17 ABS. 1

- Anspruch auf Löschung der personenbezogenen Daten bei rechtswidriger Verarbeitung, bspw.:
  - Entfallen des Verarbeitungszwecks
  - Widerruf der Einwilligung
  - Widerspruch gegen die Verarbeitung
  - Unrechtmäßige Verarbeitung
  - rechtliche Verpflichtung
  - Daten betreffen Kinder
- Dem muss nicht nachgekommen werden, wenn:
  - Recht auf freie Meinungsäußerung und Information den schutzwürdigen Interessen des Betroffenen überwiegt
  - eine rechtliche Verpflichtung dazu besteht
  - Rechtsansprüche des Verantwortlichen gegen den Betroffenen bestehen

RECHT AUF VERGESSENWERDEN ART. 17 ABS. 2

- Recht auf die Löschung von Verlinkungen, die zu personenbezogenen Daten führen (Art. 17 Abs. 2 DSGVO)
- Voraussetzung für den Anspruch auf „Vergessenwerden“
  - Öffentlichmachung durch den Verantwortlichen, jedenfalls dann gegeben, wenn die personenbezogenen Daten über gängige Suchmaschinen auffindbar sind
  - Bestehender Anspruch auf Löschung nach Art. 17 Abs. 1 DSGVO
  - Auf Verlangen des Betroffenen
- Anspruch beschränkt sich auf angemessene Maßnahmen des Verantwortlichen
- Wahrnehmung und Umsetzung nicht unterschätzen!

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG ART. 18

- Bestreiten der Richtigkeit der Daten + für die Dauer die zur Überprüfung benötigt wird
- Verarbeitung ist rechtswidrig, der Betroffene lehnt allerdings die Löschung ab und verlangt stattdessen die Einschränkung der Verarbeitung
- Ablauf der Aufbewahrungsfrist, jedoch Erforderlichkeit für Betroffenen zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen
- Bei Widerspruch nach Art. 21 – während der Prüfung der widerstreitenden Interessen

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

RECHT AUF DATENÜBERTRAGBARKEIT ART. 20

- Voraussetzung ist, dass personenbezogene Daten auf Grundlage einer Einwilligung oder eines Vertrags verarbeitet werden
- Bezieht sich nur auf Daten, die vom Betroffenen „bereitgestellt“ worden sind
  - Bei enger Auslegung nur Daten die aktiv vom Betroffenen eingegeben worden sind
  - Bei weiter Auslegung auch Daten jedweder anderer Verarbeitungsalternative aus Art. 4 Nr. 2 DSGVO
- Übermittlung an einen neuen Verantwortlichen
  - Übermittlung muss ohne Behinderung geschehen
  - Unentgeltlich
  - Keine Verpflichtung zu interorperablen Formaten
- Einrede der technischen Machbarkeit möglich
- Wahrnehmung und Umsetzung nicht unterschätzen!

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

Besonderes Augenmerk

The project is co-funded by
the REC Programme
of the European Union

BESONDERES AUGENMERK

- **Betroffenenrechte:**
  Unterschätzt welcher Aufwand sich hinter diesem Begriff verbirgt
- Es muss mitunter viel Zeit investiert werden um ein halbwegs vorzeigbares Managementsystem zu erstellen oder schlicht das Vorgehen im Fall der Fälle vorab zu strukturieren
- Viel Zeit geht durch Postwege oder „Liegenlassen“ verloren
- **Auskunftsrecht:**
  Das Paradebeispiel der Betroffenenrechte. Kunden, Verbände und Dritte überschütten Unternehmen teilweise mit der Geltendmachung des Auskunftsrechts.
- Regelmäßig nur einen Monat Zeit zum Erkennen, Bearbeiten und Antworten
- **Recht auf Löschen, Einschränkung der Verarbeitung und Datenportabilität**

Strategien?

The project is co-funded by
the REC Programme
of the European Union

STRATEGIEN?

- **Kunden/Mandanten**
  Gegenüber Kunden sollte bereits ein umfassendes Betroffenenrechte-Managementsystem oder entsprechende Regelungen vorhanden sein. Es ist zu empfehle, nach erfolgter Prüfung, den geltend gemachten Ansprüchen zu entsprechen (AUFBEWAHRUNGSFIRSTEN!). Gegenüber Mandanten muss genau geprüft und auch der Rückgriff auf § 29 BDSG-neu gewagt werden
- **Beschäftigten**
  Informieren Sie Ihre Beschäftigten gemäß Art. 13, 14 DSGVO. (Vertrag/Annex/Infoblatt)
- **Verbraucherschützer**
  Ähnlich den Kunden/Mandanten sollte das vorhandene Managementsystem verwendet und nach erfolgter Prüfung den geltend gemachten Ansprüchen entsprochen werden

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

DSGVO-Projekte

The project is co-funded by
the REC Programme
of the European Union

4-PHASEN-MODELL

- Phase 1: Bestandsaufnahme/Audit
  - Durchsicht Verfahrensverzeichnisse und ADV-Vereinbarungen
  - Ergänzung nach Bestandsaufnahme (HR, Finance, Marketing, IT)
- Phase 2: Gap-Analyse
  - Kursorische Prüfung der einzelnen Vorgänge auf DSGVO-Compliance
  - Priorisierung und Prüfung von Einzelheiten
- Phase 3: Anpassung Rechtstexte
  - Datenschutzerklärungen, etwaige Nutzungsbedingungen
  - Einwilligungserklärungen (sowohl von Kunden als auch von Mitarbeitern)
  - Standard-A(D)V-Vereinbarungen (in beide Richtungen)
- Phase 4: Datenschutzrichtlinie/Compliance
  - Fertigstellung des Verzeichnisses über die Verarbeitungstätigkeiten
  - Festlegung von Technischen und organisatorischen Maßnahmen
  - Betroffenenrechte, Datenschutzfolgeabschätzung, Meldepflichten

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

Und wir Anwälte?

The project is co-funded by
the REC Programme
of the European Union

Gute alte Zeiten…

DIE RECHTSLAGE BISLANG: § 1 ABS. 3 BDSG

„Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.“

KG VOM 20.8.2010 - 1 WS (B) 51/07 - 2 SS 23/07

„Hingegen ist hier § 1 Abs. 3 Satz 2 BDSG einschlägig. Nach dieser Bestimmung bleibt unter anderem die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten "unberührt". Danach schließen andere gesetzliche Vorschriften die Anwendung des BDSG aus, wenn sie derartige Geheimhaltungspflichten zum Gegenstand haben und den davon betroffenen Personenkreis weitergehend als im BDSG schützen (vgl. Gola/Schomerus aaO, Rdn. 25 zu § 1). Eine solche Verschwiegenheitsverpflichtung des Rechtsanwalts, die sich auf alles bezieht, was ihm in Ausübung seines Berufes bekannt geworden ist, ergibt sich aus § 43a Abs. 2 Satz 1 und 2 BRAO. Sie gehört, wie die Gesetzesüberschrift zeigt, zu den anwaltlichen Grundpflichten, die nicht nur den individuellen Belangen des Rechtsanwalts und seines Mandanten dienen, sondern auch dem öffentlichen Interesse einer wirksamen und geordneten Rechtspflege Rechnung tragen…“

Und jetzt?

ART. 90 DSGVO

„Die Mitgliedstaaten können die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber den Verantwortlichen oder den Auftragsverarbeitern, die nach Unionsrecht oder dem Recht der Mitgliedstaaten oder nach einer von den zuständigen nationalen Stellen erlassenen Verpflichtung dem Berufsgeheimnis oder einer gleichwertigen Geheimhaltungspflicht unterliegen, regeln, soweit dies notwendig und verhältnismäßig ist, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen. Diese Vorschriften gelten nur in Bezug auf personenbezogene Daten, die der Verantwortliche oder der Auftragsverarbeiter bei einer Tätigkeit erlangt oder erhoben hat, die einer solchen Geheimhaltungspflicht unterliegt.“

DIE AUSNAHMEN

• Anders als bei anderen Unternehmen haben die Aufsichtsbehörden bei Anwaltskanzleien **kein Recht auf Zugang** zu den Kanzleiräumen (§ 29 Abs. 3 BDSG-neu).

• Die Behörden haben zudem **keine Zugriffsrechte** und dürfen keine Einblicke in die anwaltliche Datenverarbeitung verlangen. Die Kanzleiserver und -rechner sind für die Behörden tabu (§ 29 Abs. 3 BDSG-neu).

• Auch bei den Betroffenenrechten gibt es Ausnahmen zum Schutz des Anwaltsgeheimnisses. Prozessgegner und andere Außenstehende können **keine Informations- und Auskunftsrechte** aus Art. 14 und 15 DSGVO geltend machen, wenn es um Daten geht, die dem Anwaltsgeheimnis unterliegen (§ 29 Abs. 1 BDSG-neu). Die Mandatsakte bleibt auf diese Weise davor geschützt, dass unter dem Deckmantel des DatenschutzrechtsAuskunft über Akteninhalte verlangt wird.

Für welche Bereiche gilt die DSGVO eigentlich?

The project is co-funded by the REC Programme of the European Union

Die DSGVO gilt für die „Verarbeitung personenbezogener Daten“. Immer wenn es um **Informationen über natürliche Personen** geht und diese Informationen in einen **Verarbeitungsvorgang** einbezogen werden, ist die DSGVO anwendbar.

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

Von einem **Verarbeitungsvorgang** spricht man

- bei einer automatisierten, **computergestützten** Verarbeitung von Daten,
- aber auch bei **Papierakten**, wenn die Akten nach einem bestimmten System oder Schema geführt werden („nach bestimmten Kriterien zugänglich sind“), und
- bei (digitalen) **Fotos** und **Videoaufnahmen**.

Die **gesamte Mandats- und Personalverwaltung** unterliegt daher dem Regelwerk der DSGVO.

Keine Anwendung findet die DSGVO

- auf handschriftliche **Notizen** und
- auf die **Telekommunikation** (Telefonate, Telefaxe, E-Mails – nur auf die Archivierung von E-Mails ist die DSGVO anwendbar).

***Personenbezug** liegt vor bei*

- *Informationen über natürliche Personen (Mandanten, Gegner, Zeugen Dritte) im Zusammenhang mit einem Mandat (**Mandatsakten**);*
- *Informationen über die Beschäftigten der Kanzlei (**Personalverwaltung und Gehaltsabrechnung**);*
- *Informationen über natürliche Personen aus der Buchhaltung (**Finanzverwaltung);***
- *Informationen über die Besucher der Website der Kanzlei (**Websitebesucher**);*
- *Informationen über die Empfänger des Newsletters der Kanzlei (**Newsletterverwaltung**);*
- *Informationen über Besucher von Veranstaltungen der Kanzlei (**Veranstaltungsmanagement**).*

SCHRITT 1

Betrieblicher Datenschutzbeauftragter

The project is co-funded by the REC Programme of the European Union

PFLICHT ZUR BESTELLUNG EINES DATENSCHUTZBEAUFTRAGTEN

- **10-Personen-Regel**: Sind mindestens zehn Personen in der Kanzlei mit der Datenverarbeitung beschäftigt, muss ein Datenschutzbeauftragter bestellt werden. Ist dies bislang nicht der Fall, sollte man die Bestellung schnellstmöglich nachholen.
- Optimal ist die Bestellung eines angestellten Anwaltes oder eines anderen Mitarbeiters mit gewisser **IT-Affinität**. Auch die Bestellung eines **externen Datenschutzbeauftragten** ist möglich. Dies ist mit § 203 StGB-neu konform.
- Für eine Datenschutzbehörde ist es leicht zu prüfen, ob eine Anwaltskanzlei einen Datenschutzbeauftragten hat, da die **Kontaktdaten** des Datenschutzbeauftragtes **in allen Datenschutzinformationen** bekannt gemacht werden und **der Behörde zudem gemeldet** werden müssen (Art. 37 Abs. 7 DSGVO).
- Der Datenschutzbeauftragte ist der Kanzleiführung direkt unterstellt, in der Wahrnehmung seiner gesetzlichen Aufgaben aber **nicht weisungsgebunden** (Art. 38 Abs. 3 DSGVO).
- Wenn der Datenschutzbeauftragte Arbeitnehmer ist, genießt er **erweiterten Kündigungsschutz** nach § 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG-neu.

SCHRITT 2

Verzeichnis über die Verarbeitungstätigkeiten

The project is co-funded by the REC Programme of the European Union

WAS IST ZU ERFASSEN?

- elektronische Anwaltsakten;
- Kanzleisoftware (zum Beispiel RA Micro, Phantasy usw.);
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware (Finanzbuchhaltung und Lohnbuchhaltung);
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- Kanzlei-Websites;
- Kanzleiseiten in Sozialen Netzwerken (z.B. Twitter, Facebook, Xing);
- elektronische Personalakten;
- betriebliches Intranet;
- Urlaubslisten

MINDESTINHALT

- Name der Datenverarbeitung (Beispiel: Lohnbuchhaltung)
- Zwecke der Datenverarbeitung (Beispiel: Lohnabrechnung)
- Beschreibung der Verarbeitung
- Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO
- Betroffene / betroffene Personengruppen (Beispiel: Arbeitnehmer)
- Personenbezogene Daten / Datenkategorien (Beispiel: Stammdaten, Kontodaten)
- Empfänger / Empfängerkategorien (Beispiel: Steuerbüro)
- Drittstaatentransfer
- Zugriffsberechtigte
- Regelfristen für die Löschung (Beispiel: 3 Jahre nach Ausscheiden des Mitarbeiters)
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

[redacted] [illegible]	Datenverarbeitung	Datenweitergabe	Eingesetzte Software und technische und organisatorische Maßnahmen	Verantwortlichkeiten [illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Tabelle1 Tabelle2 Tabelle3

B C D E F G H

nann und Partner
tungstätigkeiten nach Art. 30 DSGVO

wortliche sowie ggf.	Kanzlei Mustermann und Partner, Max-Mustermann-Straße 123, 12345 Berlin, Deutschland	**Name und Kotaktdaten des betrieblichen Datenschutzbeauftragter:**	Max Mustermann, datenschutz@xyz.de	**Zwecke**
die Daten en (intern/extern)	Hierzu zählen: Verantwortliche des öffentlichen Rechts bei Vorliegen vorrangiger Rechtsvorschriften, externe Auftragnehmer gemäß Art. 28 DSGVO sowie Dritte, soweit dies zur Erfüllung der in Spalte O genannten Zwecke erforderlich ist. Hierzu zählen Zahlungsdienstleister, Behörden, Gerichte, sonstige öffentliche Stellen. Interne Empfänger können z.B. sein: Buchhaltung, ...	**Übermittlung in Drittstaaten:**	Eine Übermittlung an andere Unternehmen mit Sitz außerhalb der EU finden nur in Ausnahmefällen und bei bestimmten Datenverarbeitungen statt. Siehe Spalte I.	**Regelfr**

Zwecke der tenverarbeitung	**Rechtsgrundlage**	**Beschreibung der Verarbeitung**	**Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO**	**Betroffene / betroffene Personengruppen**	**Personenbezogene Daten / Datenkategorien**	**Empfänger / Empfängerkategorien**	**Dri**
rung der IP-Adresse, der en Unterseiten und der auer durch die Tracking beim Besuch der Webseite. hinaus Einsatz des ool „Google Analytics“ zur ung des Webauftritts	Art. 6 Abs. 1S. 1lit. f DSGVO Art. 28 DSGVO		Nein	Webseitenbesucher	IP-Adresse der Webseitenbesucher Bewegungen und Clicks der Besucher auf der Webseite Browser-Fingerprints	**Dienstleister XY**	**Möglich**
von Newslettern	Art. 6 Abs. 1S. 1lit. a DSGVO § 7 III UWG Art. 28 DSGVO		Nein	Newsletter-Abonnenten	E-Mail-Adresse, ggf. Name	**Dienstleister XY**	**Möglich**
wartung zur Behebung von zur Verbesserung der	Wartung der Software im Auftrag bedarf keiner eigenen						

ÜBERBLICK: AUFLISTUNG DER ZU ENTHALTENEN INFORMATIONEN

- 1. Schritt: Identifizierung aller Datenverarbeitungsprozesse
- 2. Schritt : Beschreibung der Prozesse (was passiert hier genau)
  - Hier ist die Zusammenarbeit aller Abteilungen/Fachbereiche notwendig!
  - Dieser Arbeitsschritt stellt erfahrungsgemäß den Großteil der Arbeit dar.
- 3. Schritt: ggf. Zusammenfassung einzelner Prozesse zu einem
  - Dabei nicht zu kleinteilig vorgehen!
- Beschreibung der Zwecke der Verarbeitung und der betroffenen Datenkategorien
- Klärung, wer Zugriff auf die Daten hat und ob diese weitergegeben werden sollen
- Bestimmung der geplanten Aufbewahrungsfrist

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

Verzeichnis der Verarbeitungstätigkeiten der Beispiel GmbH (Art. 30 DS-GVO)

Version/Stand: ...

a1.	Namen und Kontaktdaten der Verantwortlichen sowie seines Vertreters	...
a2.	Namen und Kontaktdaten des betrieblichen Datenschutzbeauftragten	...
b.	Zwecke der Verarbeitung	Tätigkeitsgegenstand des Unternehmens ist der Fernabsatz von Waren und Diensteistungen aller Art, der Einzelhandel im Rahmen der behördlich erteilten Genehmigungen und die serienmäßige Herstellung der zum Angebot kommenden Waren. Die Datenerhebung, -verarbeitung, -übermittlung und -nutzung erfolgt zur Ausübung der zuvor genannten Zwecke. Die einzelnen Verfahren sind in der Anlage dieses Verzeichnisses im Detail beschrieben.
c.	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	Kundendaten, Mitarbeiterdaten sowie Daten von Lieferanten sowie anderer Geschäftspartner, sofern die Verarbeitung zur Erfüllung der unter b. genannten Zwecke erforderlich ist.
d.	Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden sowie Empfänger in Drittstaaten	Verantwortliche des öffentlichen Rechts bei Vorliegen vorrangiger Rechtsvorschriften, externe Auftragnehmer entsprechend Art. 28 sowie Dritte, soweit dies zur Erfüllung der unter b. genannten Zwecke erforderlich ist. Hierzu zählen Zahlungsdienstleister, Auskunfteien, Logistikunternehmen. Infolge der Einbindung von Anbietern sozialer Netzwerke erfolgt eine Verarbeitung zudem in den USA.
e.	Übermittlung in Drittstaaten	Vergleiche hierzu die Anlagen x und y.
f.	Regelfristen für die Löschung der Datenkategorien	Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn die unter b. genannten Zwecke wegfallen. Konkrete Löschfristen werden in der Anlage beschrieben.
g.	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Die Systeme der Beispiel GmbH werden durch eine Vielzahl von Maßnahmen gegen unbefugten Zugriff, Verlust oder Zerstörung und unzulässige Veränderung geschützt. Details werden in der Anlage erläutert.

Das Verfahrensverzeichnis verfügt über ... Anlagen.

BEISPIEL

ANLAGE 1

Version: ...

#	**Name des Verfahrens:**	**NEWSLETTERVERSAND**
1.	Zweckbestimmung der Datenerhebung, -verarbeitung und Nutzung	Versand von Newslettern an Interessenten und Bestandskunden
2.	Rechtsgrundlage der Datenverarbeitung	Art. 6 Abs. 1 f) DS-GVO; Art. 16 Abs. 2 E-Privacy-VO
3.	Betroffene bzw. betroffene Personengruppen	Interessenten und Bestandskunden
4.	Verwendete Datenarten bzw. -kategorien	- Vorname - Nachname - E-Mail-Adresse - ...
5.	Empfänger oder Kategorien von Empfängern, Drittstaatentransfer	Der Versand wird unter Einschaltung des Dienstleisters Mailchimp Inc. mit Sitz in Atlanta, USA durchgeführt. Mit der Mailchimp Inc. wurde ein schriftlicher Vertrag zur Auftragsdatenverarbeitung (Art. 28 DS-GVO) unter Einbeziehung der EU-Standardvertragsklauseln (2010/87/EU) abgeschlossen.
6.	Regelfrist für die Datenlöschung	Die Löschung erfolgt nach Wegfall des Zwecks der werblichen Ansprache bzw. nach erfolgtem Widerruf der Einwilligung durch die betroffene Person. Im Falle eines Werbewiderspruchs werden die Daten nach 4. in eine Werbesperrdatei überführt.
7.	Technisch-organisatorische Maßnahmen	Die interne Systeme sind wie folgt gesichert: ... Die Mailchimp Inc. ist SOC II Compliant und PCI DSS zertifiziert. Dies bedeutet ... Verschlüsselte Datenbanken, Zugriffskontrolle auf Datenbank, Zugangskontrolle zur Datenbank, ...

Löschkonzept

The project is co-funded by
the REC Programme
of the European Union

LÖSCHKONZEPT

- Für jedes Datum muss eine Löschfrist festgelegt werden
- Abhängig von der Rechtsgrundlage
  - Aufbewahrungsfristen (Steuerrecht; Handelsrecht; Berufsrecht) erleichtern die Arbeit
  - Einwilligung: Bei Befristung der Einwilligung oder Widerruf
  - Vertrag: Wenn für Vertragserfüllung und etwaigen Ansprüchen nicht mehr erforderlich
  - Berechtigte Interessen:
    - Wenn Interesse wegfällt
    - Wenn Interessen des Nutzers überwiegen

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

LÖSCHKONZEPT: VERHÄLTNIS ZU AUFBEWAHRUNGSFRISTEN

- Daten dürfen aufbewahrt werden, wenn dies gesetzlich angeordnet ist, z.B. handels- oder steuerliche Aufbewahrungspflichten
- Nur solche Daten, die von der Aufbewahrungspflicht erfasst sind
- Beispiel: Finanzbuchhaltung
  - § 147 Abs. 3 AO, zehn Jahre, beginnend mit dem Ende des Kalenderjahres, in dem das Dokument entstanden ist

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

LÖSCHKONZEPT: BEISPIELE

- Intranet
  - Daten dürfen gespeichert werden, bis Widerruf erklärt wird
  - (P) Beendigung des Arbeitsverhältnisses
- Personalakte
  - bis zum Verjährungseintritt aller absehbaren geltend zu machenden Ansprüche: 3 Jahre
- Tracking-Maßnahmen
  - § 15 TMG: maximal sieben Tage
- Newsletter
  - E-Mail-Adresse und Stammdaten: bis Widerruf
  - Daten, die aufgrund berechtigter Interessen gespeichert werden: wenige Monate

SCHRITT 3

„Gap Analysis“

The project is co-funded by
the REC Programme
of the European Union

Datenschutzprinzipien

The project is co-funded by
the REC Programme
of the European Union

DATENSCHUTZPRINZIPIEN

- Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 lit. a, 1. Fall DSGVO);
- Grundsatz der Fairness (Art. 5 Abs. 1 lit. a, 2. Fall DSGVO);
- Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a, 3. Fall DSGVO);
- Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DSGVO);
- Grundsatz der Datensparsamkeit (Art. 5 Abs. 1 lit. c DSGVO);
- Grundsatz der sachlichen Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO);
- Grundsatz der begrenzten Speicherung (Art. 5 Abs. 1 lit. e DSGVO);
- Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO);
- Grundsatz der Verantwortlichkeit (Art. 5 Abs. 2 DSGVO);
- Privacy by Design (Art. 25 Abs. 1 DSGVO);
- Privacy by Default (Art. 25 Abs. 2 DSGVO).

UND KONKRET?

- **Datenrichtigkeit**: Ist gewährleistet, dass Mandantendaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
- **Rechtmäßigkeit**: Ist die Datenverarbeitung gem. Art. 6 Abs. 1 DSGVO rechtlich zulässig? Dient die Datenverarbeitung der Erfüllung eines Vertrages? Gibt es Einwilligungen der Betroffenen? Lässt sich die Datenverarbeitung durch eigene „berechtigte Interessen“ oder durch „berechtigte Interessen“ der Mandanten legitimieren?
- **Löschfristen**: Werden Daten gelöscht, sobald sie nicht mehr benötigt werden? Gibt es eine Löschroutine, die eine rechtzeitige Löschung gewährleistet?
- **Zugriffsrechte**: Haben Mitarbeiter ausschließlich Zugriff auf Daten, die sie für ihre jeweiligen Aufgaben benötigen?
- **Zugangskontrolle**: Sind die Rechner in der Kanzlei ausreichend gegen den Zugang durch Unbefugte geschützt?
- **Schutz gegen Hacker und Malware**: Gibt es eine Firewall? Sind aktuelle Virenscanner installiert?

SCHRITT 4

Datensicherheit

The project is co-funded by
the REC Programme
of the European Union

T-O-M DATENSICHERHEIT – ART. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- **Verschlüsselung**: Es empfiehlt sich, die Verschlüsselung von E-Mails mit Verschlüsselungsprogrammen **zu ermöglichen**.
- **Stabilität:** Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme ist auf Dauer sicherzustellen. Hierzu bedarf es einer fachkundigen Einschätzung einer IT-Fachfirma oder eines fachkundigen Mitarbeiters.
- **Wiederherstellbarkeit:** Verarbeitungsprozesse müssen gegen Datenverlust geschützt werden durch eine fachgerechte Datensicherung. Auch hierzu bedarf es der Unterstützung durch IT-Fachleute.
- **Regelmäßige Überprüfung:** Eine regelmäßige Routineprüfung ist für die Datensicherheit gleichfalls vorgeschrieben.

Technische und organisatorische Maßnahmen der Datensicherheit

DAV-Muster als Checkliste

Art. 32 DSGVO verpflichtet jede Kanzlei zu Maßnahmen, die die Integrität und Vertraulichkeit der Datenverarbeitung gewährleisten. Dieses Muster ist als „Checkliste" gedacht. Die Punkte, die in diesem Muster genannt sind, sollten mit einem IT-Fachmann besprochen werden. Das Ziel der Besprechung sollte es sein, einen Bericht zu erstellen, der die Maßnahmen dokumentiert, die die Kanzlei zur Datensicherheit ergriffen hat. Sollten sich aus dem Gespräch Vorschläge ergeben zur verbesserten Sicherheit – umso besser. Die Checkliste lautet:

1. Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird.
Zum Beispiel:
- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke
- Sorgfältige Auswahl Reinigungspersonal
- Sicherheitsschlösser

2. Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können.
Zum Beispiel:
- Sichere Aufbewahrung von Datenträgern
- Einrichtungen von Standleitungen beziehungsweise VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

3. Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.
Zum Beispiel:
- Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

ziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

4. Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzten können.
Zum Beispiel:
- Festlegung zugangsberechtigter Mitarbeiter
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von Verschlüsselungs-Technologie
- Einsatz von Anti-Viren-Software

5. Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.
Zum Beispiel:
- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

6. Übertragungskontrolle

Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.
Zum Beispiel:
- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

7. Transportkontrolle

SCHRITT 5

Informationspflichten

The project is co-funded by
the REC Programme
of the European Union

DAV-Muster: Datenschutzerklärung für Kanzleiwebsite

DAV-Muster umfasst auch Social Media und Analyse Tools

Dieses Muster dient dazu, für die Kanzlei-Website die Anforderungen der Art. 13 und 14 DSGVO (Informationspflichten) zu erfüllen. Hierbei geht es nur um die Datenverarbeitungsprozesse, die mit dem Besuch der Website verbunden sind. Es gibt keine Besonderheiten für Anwälte, da eine Kanzlei-Website nicht anders funktioniert als Websites anderer Unternehmen. Das Muster geht von einer anspruchsvollen Gestaltung der Website aus, die beispielsweise Verknüpfungen zu Social Media und die Nutzung von Analyse-Tools umfasst. Bei einfacheren Internetauftritten lässt sich das Muster erheblich kürzen. Das DAV-Muster einer Datenschutzerklärung für die Kanzleiwebsite lautet:

1. Name und Kontaktdaten des für die Verarbeitung Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten

Diese Datenschutz-Information gilt für die Datenverarbeitung durch:

Verantwortlicher: XY Rechtsanwälte (im Folgenden: XY), Littenstraße 11, D-10179 Berlin, Deutschland
Email: _____@xyrecht.de
Telefon: +49 (0)30 – XXXXXX
Fax: +49 (0)30 – XXXXXX

Der/die betriebliche Datenschutzbeauftragte von XY ist unter der o.g. Anschrift, zu Hd. Herrn Mustermann, beziehungsweise unter _____@xyrecht.de erreichbar.

2. Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck von deren Verwendung

a) Beim Besuch der Website

Beim Aufrufen unserer Website **www.xyrechtsanwaelte.de** werden durch den auf Ihrem Endgerät zum Einsatz kommenden Browser automatisch Informationen an den Server unserer Website gesendet. Diese Informationen werden temporär in einem sog. Logfile gespeichert. Folgende Informationen werden dabei ohne Ihr Zutun erfasst und bis zur automatischen

- Auswertung der Systemsicherheit und -stabilität sowie
- zu weiteren administrativen Zwecken.

Die Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 S. 1 lit. f DSGVO. Unser berechtigtes Interesse folgt aus oben aufgelisteten Zwecken zur Datenerhebung. In keinem Fall verwenden wir die erhobenen Daten zu dem Zweck, Rückschlüsse auf Ihre Person zu ziehen.

Darüber hinaus setzen wir beim Besuch unserer Website Cookies sowie Analysedienste ein. Nähere Erläuterungen dazu erhalten Sie unter den Ziff. 4 und 5 dieser Datenschutzerklärung.

b) Bei Anmeldung für unseren Newsletter

Sofern Sie nach Art. 6 Abs. 1 S. 1 lit. a DSGVO ausdrücklich eingewilligt haben, verwenden wir Ihre E-Mail-Adresse dafür, Ihnen regelmäßig unseren Newsletter zu übersenden. Für den Empfang des Newsletters ist die Angabe einer E-Mail-Adresse ausreichend.

Die Abmeldung ist jederzeit möglich, zum Beispiel über einen Link am Ende eines jeden Newsletters. Alternativ können Sie Ihren Abmeldewunsch gerne auch jederzeit an _____@xyrecht.de per E-Mail senden.

c) Bei Nutzung unseres Kontaktformulars

Bei Fragen jeglicher Art bieten wir Ihnen die Möglichkeit, mit uns über ein auf der Website bereitgestelltes Formular Kontakt aufzunehmen. Dabei ist die Angabe einer gültigen E-Mail-Adresse erforderlich, damit wir wissen, von wem die Anfrage stammt und um diese beantworten zu können. Weitere Angaben können freiwillig getätigt werden.

Die Datenverarbeitung zum Zwecke der Kontaktaufnahme mit uns erfolgt nach Art. 6 Abs. 1 S. 1 lit. a DSGVO auf Grundlage Ihrer freiwillig erteilten Einwilligung.

Die für die Benutzung des Kontaktformulars von uns erhobenen personenbezogenen Daten werden nach Erledigung der von Ihnen gestellten Anfrage automatisch gelöscht.

3. Weitergabe von Daten

Eine Übermittlung Ihrer persönlichen Daten an Dritte zu anderen als den im Folgenden aufgeführten Zwecken findet nicht statt.

Wir geben Ihre persönlichen Daten nur an Dritte weiter, wenn:

- Sie Ihre nach Art. 6 Abs. 1 S. 1 lit. a DSGVO ausdrückliche Einwilligung dazu erteilt haben,
- die Weitergabe nach Art. 6 Abs. 1 S. 1 lit. f DSGVO zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist und kein Grund zur Annahme besteht, dass Sie ein überwiegendes schutzwürdiges Interesse

DAV-Muster: Hinweise zur Datenverarbeitung

Einfaches Muster zur Erfüllung der Informationspflichten bei Mandatsbeginn

Dies ist ein einfaches Muster zur Erfüllung der Informationspflichten, die sich bei Mandatsbeginn aus Art. 13 und 14 DSGVO ergeben. Je nach der Art des Mandats können Verpflichtungen zu weiteren Informationen bestehen, beispielsweise wenn sensible Daten verarbeitet werden (Art. 9 DSGVO) oder wenn ein Datentransfer in Nicht-EU-Staaten beabsichtigt ist (Art. 44 ff. DSGVO). Der DAV schlägt das folgende Muster vor:

Hinweise zur Datenverarbeitung

1. Name und Kontaktdaten des für die Verarbeitung Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten

Diese Datenschutzhinweise gelten für die Datenverarbeitung durch:

Verantwortlicher: XY Rechtsanwälte (im Folgenden: XY), Littenstraße 11, D-10179 Berlin, Deutschland
Email: _____@xyrecht.de
Telefon: +49 (0)30 – XXXXXX
Fax: +49 (0)30 – XXXXXX

Der/die betriebliche Datenschutzbeauftragte von XY ist unter der o.g. Anschrift, zu Hd. Herrn Mustermann, beziehungsweise unter _____@xyrecht.de erreichbar.

2. Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck und deren Verwendung

Wenn Sie uns mandatieren, erheben wir folgende Informationen:

- Anrede, Vorname, Nachname,
- eine gültige E-Mail-Adresse,
- Anschrift,
- Telefonnummer (Festnetz und/oder Mobilfunk)
- Informationen, die für die Geltendmachung und Verteidigung Ihrer Rechte im Rahmen des Mandats notwendig sind

Die Erhebung dieser Daten erfolgt,

- um Sie als unseren Mandanten identifizieren zu können;
- um Sie angemessen anwaltlich beraten und vertreten zu können;

Die für die Mandatierung von uns erhobenen personenbezogenen Daten werden bis zum Ablauf der gesetzlichen Aufbewahrungspflicht für Anwälte (6 Jahre nach Ablauf des Kalenderjahres, in dem das Mandat beendet wurde,) gespeichert und danach gelöscht, es sei denn, dass wir nach Artikel 6 Abs. 1 S. 1 lit. c DSGVO aufgrund von steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten (aus HGB, StGB oder AO) 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.

3. Weitergabe von Daten an Dritte

Eine Übermittlung Ihrer persönlichen Daten an Dritte zu anderen als den im Folgenden aufgeführten Zwecken findet nicht statt.

Soweit dies nach Art. 6 Abs. 1 S. 1 lit. b DSGVO für die Abwicklung von Mandatsverhältnissen mit Ihnen erforderlich ist, werden Ihre personenbezogenen Daten an Dritte weitergegeben. Hierzu gehört insbesondere die Weitergabe an Verfahrensgegner und deren Vertreter (insbesondere deren Rechtsanwälte) sowie Gerichte und andere öffentliche Behörden zum Zwecke der Korrespondenz sowie zur Geltendmachung und Verteidigung Ihrer Rechte. Die weitergegebenen Daten dürfen von dem Dritten ausschließlich zu den genannten Zwecken verwendet werden.

Das Anwaltsgeheimnis bleibt unberührt. Soweit es sich um Daten handelt, die dem Anwaltsgeheimnis unterliegen, erfolgt eine Weitergabe an Dritte nur in Absprache mit Ihnen.

4. Betroffenenrechte

Sie haben das Recht:

- gemäß Art. 7 Abs. 3 DSGVO Ihre einmal erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf dieser Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen;
- gemäß Art. 15 DSGVO Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten zu verlangen. Insbesondere können Sie Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen;
- gemäß Art. 16 DSGVO unverzüglich die Berichtigung unrichtiger oder Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen;
- gemäß Art. 17 DSGVO die Löschung Ihrer bei uns gespei-

INFORMATIONSPFLICHTEN

- **Identität der verantwortlichen Stelle**: Neu sind die vorgeschriebenen Angaben zur Identität und den Kontaktdaten eines Vertreters (Art. 27 DSGVO) und zur Identität (nicht: Kontaktdaten) des betrieblichen Datenschutzbeauftragten.
- **Art der Daten**: Werden die Daten nicht bei dem Betroffenen erhoben (Art. 14 DSGVO), ist eine Angabe zu der Art der Daten vorgeschrieben, die verarbeitet werden sollen.
- **Zweckbestimmung:** Neu ist die vorgeschriebene Angabe zur Rechtsgrundlage der Datenverarbeitung. Der Datenverarbeiter muss sich in der Datenschutzerklärung festlegen, auf welche der Erlaubnisse gemäß Art. 6 DSGVO er die Datenverarbeitung stützen möchte.
- **Empfänger**: Wenn eine Übermittlung personenbezogener Daten an Dritte beabsichtigt ist, sind die konkreten Empfänger anzugeben. Steht noch nicht fest, wer die Empfänger konkret sein werden, genügen Angaben zur Kategorie der Empfänger (z.B. „Weitergabe an Werbepartner“; „Weitergabe an Versandunternehmen“; „Weitergabe an andere Unternehmen im selben Konzern“).

INFORMATIONSPFLICHTEN

- **Freiwilligkeit** (nur wenn Daten bei dem Betroffenen erhoben werden, Art. 13 DSGVO): Der Betroffene ist darauf hinzuweisen, ob er gesetzlich oder vertraglich zur Bereitstellung personenbezogener Daten verpflichtet ist oder ob die Bereitstellung der personenbezogenen Daten für einen Vertragsschluss erforderlich ist. Zudem bedarf es einer Belehrung über die möglichen Folgen einer verweigerten Bereitstellung.
- **Datentransfer in Drittstaaten**: Über die beabsichtigte Übermittlung von personenbezogenen Daten in einen Staat außerhalb der EU ist stets zu informieren. Es bedarf zudem einer Angabe, auf welche Rechtsgrundlage sich der Verantwortliche bei dem Datentransfer gemäß Art. 44 ff. DSGVO stützen möchte. Möchte er den Datentransfer beispielsweise auf Standardvertragsklauseln oder Binding Corporate Rules (BCR) stützen, bedarf es zudem einer Kopie der Klauseln bzw. der BCR oder einer Quellenangabe, die dem Betroffenen den Einblick in die Klauseln bzw. die BCR ermöglicht.

INFORMATIONSPFLICHTEN

- **Einwilligung**: Möchte der Verantwortliche den Verarbeitungsprozess auf Einwilligungen der Betroffenen stützen, muss er die Betroffenen auf die Widerruflichkeit der Einwilligung hinweisen. Zudem bedarf es der Belehrung, dass ein Widerruf nichts an der Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung ändert (keine Rückwirkung des Widerrufs).
- **Berechtigtes Interesse**: Möchte der Verantwortliche den Verarbeitungsprozess auf berechtigte Interessen gemäß Art. 6 Abs. 1 Satz 1 lit. f DSGVO stützen, muss er angeben, um welche Interessen es sich handelt.
- **Speicherdauer**: Vorgeschrieben sind Angaben zur Speicherdauer personenbezogener Daten. Ist dies nicht möglich, müssen die Kriterien angegeben werden, nach denen sich die Speicherdauer bestimmt.

INFORMATIONSPFLICHTEN

- **Betroffenenrechte**: Die Betroffenen sind auf ihre Rechte auf Zugang, Berichtigung, Sperrung, Löschung, Widerspruch und Datenübertragbarkeit (Art. 15 bis 21 DSGVO) hinzuweisen.
- **Profiling**: Wenn ein Profiling oder eine andere Art von automatisierter Einzelfallentscheidung gemäß Art. 22 DSGVO beabsichtigt ist, ist hierauf hinzuweisen. Zudem bedarf es sinnhafter Angaben zur verwendeten „Logik“ und eines Hinweises auf die Bedeutung und die beabsichtigten Konsequenzen des Profiling für den Betroffenen.
- **Beschwerderecht**: Es bedarf eines Hinweises auf das Beschwerderecht der Betroffenen bei einer Aufsichtsbehörde (Art. 77 Abs. 1 DSGVO).
- **Herkunft der Daten** (nur bei Daten, die nicht bei dem Betroffenen erhoben werden, Art. 14 DSGVO): Der Datenverarbeiter muss die Quellen offenlegen, aus denen die Daten stammen. Handelt es sich um öffentlich zugängliche Quellen, ist dies gleichfalls anzugeben.

Datenschutz-Grundverordnung: Jede Kanzlei muss handeln

Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung (DSGVO) in Kraft. Sie gilt auch für Anwaltskanzleien. Damit sich jede Kanzlei darauf vorbereiten kann, stellt der DAV Merkblatt, Muster und Checkliste bereit.

Anwaltskanzleien sollten das neue europäische Datenschutzrecht ernst nehmen, weil die Datenschutzbehörden auf Beschwerden von Mandanten, Mitarbeitern, Prozessgegnern und anderen Dritten mit förmlichen Verfahren reagieren müssen. Die Datenschutzbehörden halten sich zudem für verpflichtet, empfindliche Bußgelder zu verhängen, wenn Datenschutzverstöße festgestellt werden.

In fünf Schritten zur Datenschutz-Grundverordnung

Alles Wichtige zum neuen Recht fasst das DAV-Merkblatt zusammen.

Fünf Schritte helfen bei der Umsetzung der Datenschutz-Grundverordnung. Dazu gibt es die folgenden Muster:

- Hinweise zur Datenverarbeitung (zur Übergabe bei Mandatsbeginn).
- Datenschutzerklärung (für die Kanzlei-Website).
- Technische und organisatorische Maßnahmen der Datensicherheit (zur Dokumentation und zur Vorlage bei Überprüfungen)
- DAV-Musterverzeichnis der Verarbeitungstätigkeiten (xls) nach Art. 30 DSGVO (zur Dokumentation und zur Vorlage bei Überprüfungen).

Downloads

DAV-Merkblatt: Umsetzung der Datenschutz-Grundverordnung in Anwaltskanzleien (PDF, 197,8 kB)

DAV-Muster: Hinweise zur Datenverarbeitung (PDF, 98,0 kB)

DAV-Muster: Datenschutzerklärung für Kanzleiwebsite (PDF, 180,0 kB)

Technische und organisatorische Maßnahmen der Datensicherheit (PDF, 104,4 kB)

DAV_Muster-Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO (XLSX, 18,8 kB)

Und zum Mitschreiben:

https://anwaltverein.de/de/praxis/datenschutz

FAQ zur DSGVO

The project is co-funded by the REC Programme of the European Union

Müssen wir nicht unabhängig von der Kopfzahl einen Datenschutzbeauftragten bestellen, weil unser Schriftverkehr besonders sensibel ist?

The project is co-funded by the REC Programme of the European Union

- Unabhängig von der Kopfzahl muss nach Art. 37 Abs. 1 lit. c DSGVO ein Datenschutzbeauftragter bestellt werden, wenn „die **Kerntätigkeit** … in der umfangreichen **Verarbeitung besonderer Kategorien von Daten** gemäß Art. 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 besteht.“

- Kanzleien verarbeiten zwar sensible Daten, die durch Art. 9 und 10 DSGVO besonders geschützt sind. Die **„Kerntätigkeit“ einer Kanzlei** liegt jedoch in der **Rechtsberatung und Rechtsvertretung** und nicht in der Verarbeitung sensibler Daten. Für Arztpraxen, bei denen sich dieselbe Frage stellt, haben mehrere Aufsichtsbehörden diese Lesart des Art. 37 Abs. 1 lit. c DSGVO bereits bestätigt.

Müssen wir E-Mails verschlüsseln?

The project is co-funded by the REC Programme of the European Union

- **Keine Verschlüsselungspflicht:** Art. 32 DSGVO verpflichtet nicht dazu, Personendaten durchgängig und ausnahmslos zu verschlüsseln. Art. 32 DSGVO ist zudem keine Verpflichtung zur Verschlüsselung von E-Mails zu entnehmen.
- Art. 32 DSGVO verpflichtet zu einer **Risikobewertung**. E-Mail-Verkehr, in dem es um Krankheiten von Mandanten geht, fällt in eine andere Risikostufe als die Mitteilung einer gerichtlichen Fristverlängerung. Je heikler die Inhalte einer Mail, desto eher besteht Anlass, über eine Verschlüsselung oder Pseudonymisierung nachzudenken. Wenn man Informationen versendet, die einen Briefumschlag mit der Aufschrift „Persönlich/Vertraulich/Verschlossen“ verdienen, verbietet es sich, die Nachricht per unverschlüsselter Mail zu versenden, ohne zuvor den Empfänger um Erlaubnis zu bitten.

Müssen wir die Informationspflichten nur gegenüber neuen Mandanten und Mitarbeitern beachten und müssen wir alle Mandanten und Mitarbeiter „nachinformieren“?

The project is co-funded by the REC Programme of the European Union

- Informationspflichten entstehen nach der DSGVO zum Zeitpunkt der Datenerhebung. Für Daten, die die Kanzleien vor dem 25.5.2018 erhoben haben, sieht die DSGVO keine nachträglichen oder rückwirkenden Informationspflichten vor. Daher ist es gut vertretbar, **auf eine „Nachinformation“ von Mandanten und Beschäftigten zu verzichten**, soweit es um die Verarbeitung von Daten geht, die bereits vor dem 25.5.2018 erhoben wurden.

- Mit jeder neuen Datenerhebung entsteht allerdings eine Verpflichtung zur Information. Teilt daher ein Mandant beispielsweise eine Adressänderung mit, sollte dem Mandanten die „Hinweise zur Datenverarbeitung“ mitgeteilt werden. Um einen fehlerfreien Informationsfluss zu gewährleisten, dürfte es sich daher anbieten, die zu erstellenden **„Hinweise zur Datenverarbeitung“** allen Mandanten und Mitarbeitern ohne Rücksicht auf deren Eintrittsdatum zur Verfügung zu stellen.

Was ist bei Dienstleistern zu beachten?

The project is co-funded by
the REC Programme
of the European Union

Achtung Berufsrecht

§ 43e BRAO - Inanspruchnahme von Dienstleistungen

Stand: 02.04.2018

Dritter Teil (Rechte und Pflichten des Rechtsanwalts und berufliche Zusammenarbeit der Rechtsanwälte)
Erster Abschnitt (Allgemeines)

(1) Der Rechtsanwalt darf Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung zur Verschwiegenheit gemäß § 43a Absatz 2 Satz 1 bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Dienstleister ist eine andere Person oder Stelle, die vom Rechtsanwalt im Rahmen seiner Berufsausübung mit Dienstleistungen beauftragt wird.

(2) Der Rechtsanwalt ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Er hat die Zusammenarbeit unverzüglich zu beenden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.

(3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist

1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.

Zusammenarbeit unverzüglich zu beenden, wenn die Einhaltung der dem Dienstleister gemäß Absatz 3 zu machenden Vorgaben nicht gewährleistet ist.

(3) Der Vertrag mit dem Dienstleister bedarf der Textform. In ihm ist

1. der Dienstleister unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten,
2. der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und
3. festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.

(4) Bei der Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen unbeschadet der übrigen Voraussetzungen dieser Vorschrift nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.

(5) Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat dienen, darf der Rechtsanwalt dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat.

(6) Die Absätze 2 und 3 gelten auch im Fall der Inanspruchnahme von Dienstleistungen, in die der Mandant eingewilligt hat, sofern der Mandant nicht ausdrücklich auf die Einhaltung der in den Absätzen 2 und 3 genannten Anforderungen verzichtet hat.

(7) Die Absätze 1 bis 6 gelten nicht, soweit Dienstleistungen auf Grund besonderer gesetzlicher Vorschriften in Anspruch genommen werden. Absatz 3 Satz 2 gilt nicht, soweit der Dienstleister hinsichtlich der zu erbringenden Dienstleistung gesetzlich zur Verschwiegenheit verpflichtet ist.

(8) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

WAS IST AUFTRAGSVERARBEITUNG?

- Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
  - **Auftraggeber bestimmt die Zwecke**
  - **Auftragnehmer ist weisungsgebunden**
- **Vertragstyp** des Auftragsverhältnisses ist **unerheblich**, allerdings muss die Datenverarbeitung den Schwerpunkt darstellen

ABGRENZUNG: GEMEINSAME VERANTWORTUNG - „JOINT CONTROL“ ?

- Verantwortlicher ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 Hs. 1 DSGVO)
- Bei gemeinsamer Verarbeitung gleichberechtigte Verantwortung und Haftung (Art. 26 DSGVO „Joint Control“)
- Vertragsschluss erforderlich, vor allem zu den Betroffenenrechten

Niko Härting | HÄRTING Rechtsanwälte | haerting@haerting.de
Lasse Konrad | HÄRTING Rechtsanwälte | konrad@haerting.de

PFLICHTEN DES VERANTWORTLICHEN

- Auswahl eines tauglichen Auftragsverarbeiters (Art. 28 Abs. 1 DSGVO), keine fortwährende Überprüfungspflicht
- Kontrollrechte (Art. 28 Abs. 3 S. 1,2 DSGVO)
- Durchführung geeigneter Datenschutzvorkehrungen (Art. 24 Abs.2 DSGVO)
- Umsetzung geeigneter technischer und organisatorischer Maßnahmen (Art. 24 Abs. 1 DSGVO)
  - DSGVO: Garantien für geeignete TOM‘s, somit keine direkte Kontrollpflicht mehr (Art. 28 Abs. 1 DSGVO)
- Führung eines schriftlichen oder elektronischen Verfahrensverzeichnisses (Art. 30 Abs. 1, 3 DSGVO)

ANFORDERUNGEN AN DEN AV-VERTRAG

- Anforderungen aus Art. 28 Abs. 3 DSGVO
- Verarbeitung kann auf Grund eines Vertrags oder eines anderen Rechtsinstruments erfolgen
  - Vertrag soll die Bindung des Auftragsverarbeiters an den Verantwortlichen rechtlich verbindlich dokumentieren und eine Verarbeitung nach den Prinzipien der DSGVO gewährleisten
  - Muss schriftlich oder in elektronischer Form geschlossen werden (Art. 28 Abs. 9 DSGVO)
- Technische und organisatorische Fragen bleiben dem Auftragsverarbeiter überlassen (Art. 28 Abs. 1 DSGVO)
  - Verantwortlicher muss lediglich zu Beginn der Auftragsverarbeitung sicherstellen, dass geeignete TOMs vorhanden sind
- Bei Verstoß gegen die Regelungsvorgaben ist die Auftragsdatenverarbeitung mangels Rechtsgrundlage unwirksam und der Verarbeitende wird zum Dritten

Brauchen wir für jede Verarbeitung von Personendaten eine Einwilligung?

The project is co-funded by the REC Programme of the European Union

Entgegen einem weitverbreiteten Missverständnis erfordert die Datenverarbeitung nach der DSGVO nicht in jedem Fall einer Einwilligung. Ebenso wenig ist eine Einwilligung regelmäßig erforderlich, wenn personenbezogene Daten verarbeitet werden sollen. Die **Einwilligung** ist nicht mehr als **eine von sechs alternativen Erlaubnistatbeständen**, die sich in Art. 6 Abs. 1 Satz 1 DSGVO finden.

Für Kanzleien von Bedeutung sind insbesondere die Tatbestände der **Vertragserfüllung und –vorbereitung** (Art. 6 Abs. 1 Satz 1 lit. b DSGVO) und der **berechtigten Interessen** (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Die meisten Verarbeitungsprozesse lassen sich auf eine dieser Grundlagen stützen:

- **Mitarbeiter:** Die Verarbeitung von Mitarbeiterdaten dient in aller Regel der Erfüllung des Arbeitsvertrages und lässt sich daher ohne weiteres auf Art. 6 Abs. 1 Satz 1 lit. b DSGVO stützen (vgl. auch § 26 BDSG).
- **Mandanten:** Soweit die Datenverarbeitung zur Bearbeitung des Mandates erforderlich ist, liegt gleichfalls ein Fall der Vertragserfüllung vor, sodass die Datenverarbeitung nach Art. 6 Abs. 1 Satz 1 lit. b DSGVO rechtmäßig ist.
- **Nichtmandanten (Dritte):** Auch die Verarbeitung von Personendaten eines Dritten bedarf keineswegs stets der Einwilligung des Betroffenen. Vielfach lässt sich eine Datenverarbeitung auf den Erlaubnisgrund der (überwiegenden) **berechtigten Interessen** an einer Datenverarbeitung stützen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Ein berechtigtes Interesse kann laut Erwägungsgrund 47 DSGVO die **Direktwerbung** sein.

Dürfen wir Adressen von Dritten ohne deren Einwilligung speichern und für Einladungen und andere Werbezwecke verwenden?

The project is co-funded by the REC Programme of the European Union

- Nach der DSGVO kann die **Direktwerbung** ein berechtigtes Interesse sein, das eine Speicherung und Nutzung von Adressdaten zu Werbezwecken legitimiert (Art. 6 Abs. 1 Satz 1 lit. f und Erwägungsgrund 47 DSGVO). Es bedarf daher **keiner Einwilligung**. Dies gilt ganz **unabhängig von der Quelle**, aus der die Adressdaten stammen. Ob ein befreundeter Kollege die Daten zur Verfügung gestellt hat oder ob die Daten das Ergebnis einer eigenen Internetrecherche sind, die Speicherung und Verwendung der Daten ist durch Art. 6 Abs. 1 Satz 1 lit. f und Erwägungsgrund 47 DSGVO gedeckt.
- Zu beachten ist das **jederzeitige Widerspruchsrecht** des Empfängers von Direktwerbung, das sich aus Art. 21 Abs. 2 DSGVO ergibt. Geht bei der Kanzlei ein Widerspruch ein, so darf die Adresse ab sofort nicht mehr zu Werbezwecken verwendet werden (Art. 21 Abs. 3 DSGVO). Wird die Adresse ausschließlich zu Werbezwecken gespeichert, so muss sie in der Adressdatenbank gelöscht werden.
- Gegenüber dem Dritten bestehen zudem die **Informationspflichten** gemäß Art. 14 DSGVO, zu denen auch eine Information über das Widerspruchsrecht zählt.

Für die **E-Mail-Werbung** bleibt es bei den unveränderten Maßgaben des Art. 7 Abs. 2 Nr. 3 UWG. Wie bisher darf daher per E-Mail nur geworben werden, wenn der Empfänger **eingewilligt** hat. Gibt es Streit über die Einwilligung, muss die Kanzlei nachweisen, dass die Einwilligung im **Double-Opt-In-Verfahren** eingeholt wurde. Erst wenn eine Einwilligung vom Adressaten noch einmal ausdrücklich bestätigt wurde („Double-Opt-In“), lässt sich die Adresse rechtssicher für E-Mail-Werbung verwenden.

Was gilt nach der DSGVO für Newsletter?

The project is co-funded by the REC Programme of the European Union

- Die DSGVO bringt keine wesentlichen Änderungen für Newsletter. Es bleibt bei dem Einwilligungserfordernis nach § 7 Abs. 2 Nr. 3 UWG. Die Einwilligung ist im Streitfall nur durch ein dokumentiertes **Double-Opt-In-Verfahren** nachweisbar.
- § 7 Abs. 2 Nr. 3 UWG beruht auf der europäischen E-Privacy-Richtlinie aus dem Jahre 2002. Dort sind keine Bußgelder vorgesehen. Die Datenschutzbehörden sind für die Ahndung von Verstößen gegen § 7 Abs. 2 Nr. 3 UWG nicht zuständig und können bei Verstößen **keine Bußgelder** verhängen.
- Für die E-Mail-Adresse, die bei der Anmeldung zum Newsletter erhoben wird, gelten die Informationspflichten gemäß Art. 13 DSGVO. Daher empfiehlt es sich, in die Website-Datenschutzerklärung Informationen über den Newsletter aufzunehmen und in das Formular für die Newsletter-Anmeldung einen **Link zu der Datenschutzerklärung** aufzunehmen.

Brauchen wir für die Verteilung von Teilnehmerlisten bei Veranstaltungen die Einwilligung der Teilnehmer?

The project is co-funded by the REC Programme of the European Union

- Die Einholung von **Einwilligungen** ist **ratsam**, da sich die Verteilung der Teilnehmerlisten nicht auf eine Notwendigkeit der Datenerhebung zur Vertragserfüllung stützen lässt (Art. 6 Abs. 1 Satz 1 lit. b DSGVO). Es erscheint zwar vertretbar, von einer Zulässigkeit kraft berechtigter Interessen auszugehen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO), da es im Interesse aller Teilnehmer liegt, Informationen über die anderen Teilnehmer zu erhalten. Hier wird man jedoch auch die gegenteilige Auffassung vertreten können, sodass die Einholung von Einwilligungen der **sicherere Weg** ist für eine rechtmäßige Aufnahme der Namen und Adressen in die Teilnehmerlisten.
- In Datenschutzinformationen, die in Form eines „**Merkblatts**“ bei Einholung der Einwilligung mitgeteilt werden können, sind die Pflichtangaben nach Art. 13 DSGVO aufzunehmen. Hierzu gehört auch der Hinweis auf die jederzeitige **Widerruflichkeit** der Einwilligung.

Was gilt in Zukunft für Fotos? Müssen wir Veranstaltungsgäste um Erlaubnis bitten, wenn wir auf unserer Websites über die Veranstaltung mit Fotos berichten möchten?

The project is co-funded by the REC Programme of the European Union

- Nach Art. 7 Abs. 3 DSGVO ist jede Einwilligung frei und mit sofortiger Wirkung widerruflich. Dies kann bei Veranstaltungsfotos auf Websites und in gedruckten Publikationen eine erhebliche Herausforderung darstellen. Daher erscheint es ratsam, **auf Einwilligungen** zu **verzichten** und stattdessen die Anfertigung und Veröffentlichung der Fotos auf den Tatbestand **berechtigter Interessen** zu stützen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO). Das Interesse der Kanzlei, unter Nutzung von Fotos von einer eigenen Veranstaltung zu berichten, ist legitim. Der Eingriff in Persönlichkeitsrechte wiegt dagegen nicht allzu schwer, da die Fotos nicht in privater Umgebung, sondern bei einem (kanzlei-)öffentlichen Ereignis angefertigt werden.

- In Datenschutzinformationen, die in Form eines „**Merkblatts**“ bei der Anmeldung zur Veranstaltung mitgeteilt werden können, sind zu den Fotos die Pflichtangaben nach Art. 13 und 14 DSGVO aufzunehmen. Hierzu gehört auch der Hinweis auf das Widerspruchsrecht der Teilnehmer nach Art. 21 Abs. 1 DSGVO.

- Das Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO unterscheidet sich erheblich von dem Recht auf Widerruf der Einwilligung, da es sich um **kein freies Widerspruchsrecht** handelt. Vielmehr bedarf es eines wichtigen Grundes (einer „besonderen Situation“), damit infolge des Widerspruchs die weitere Verbreitung eines Fotos unzulässig wird.

HÄRTING

Prof. Niko Härting
Rechtsanwalt
twitter.com/nhaerting

Lasse Konrad
Rechtsanwalt
twitter.com/LasseKonrad

HÄRTING Rechtsanwälte
Chausseestraße 13, 10115 Berlin
Tel. +49 30 28 30 57 40
Fax. +49 30 28 30 57 44

www.haerting.de