Datenschutz-Grundverordnung

Was Sie 2017 in Ihrem Unternehmen anpacken sollten

Dr. Axel von Walter
Rechtsanwalt – Fachanwalt für Urheber- und Medienrecht
Fachanwalt für Informationstechnologierecht

BEITEN BURKHARDT

Agenda

I. Anforderungen an Ihr Unternehmen

II. Implementierung

III. Roadmap

Kurze Standortbestimmung

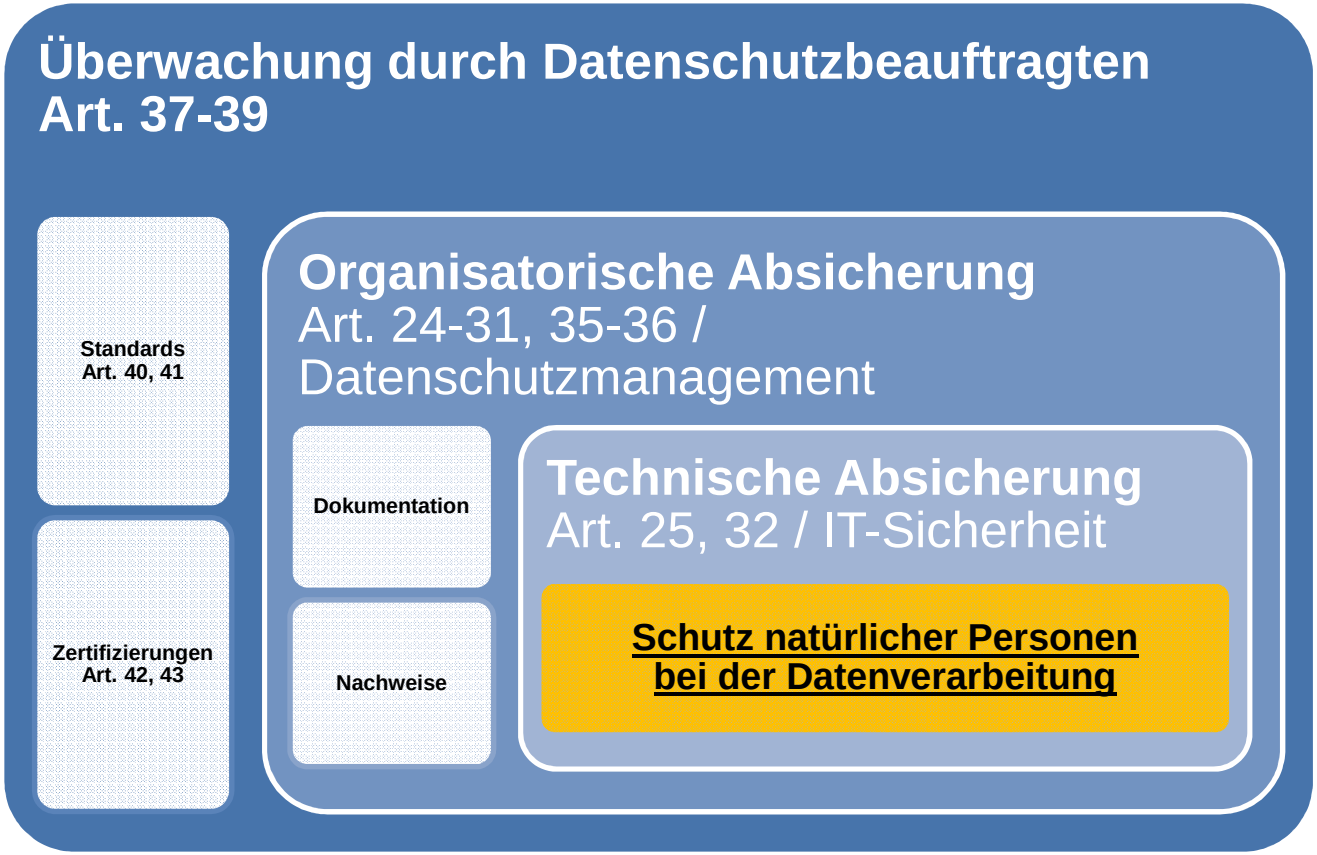
Zieldatum: 25. Mai 2018

- Was passiert bis dahin?
- Was machen andere Unternehmen?
- Was macht der Gesetzgeber?
- Was machen die Behörden?
  - Nationale Aufsichtsbehörden
  - Art. 29 Gruppe (EU)
  - Andere Mitgliedstaaten

Anforderungen an Ihr Unternehmen

BEITEN BURKHARDT

I. Anforderungen – Schutzmodell der DSGVO



Nach: Gola et al.: Datenschutzgrundverordnung im Überblick, 2017

I. Anforderungen – Überblick

Verantwortlichkeit / „Accountability“	Verarbeitungs-verzeichnis	Datenschutz-Folgenschätzung	ToM: „Privacy by Design and by Default“
Datenschutz-organisation	Datenschutz-kommunikation	Löschkonzept	Datensicherheit
Data Breach	Verträge und Einwilligungen	Transparenz / Betroffenenrechte	Internationaler Datentransfer

I. Anforderungen – Verantwortlichkeit / „*Accountability*“

- Der Verantwortliche ist verantwortlich, dass Datenverarbeitung im Einklang mit DSGVO steht und muss dies nachweisen können (Art. 5 Abs. 2, vgl. auch Art. 24 Abs. 1).
- Weitere speziellere Nachweis- und Dokumentations-pflichten

Notwendige Maßnahmen:

- technische und organisatorische Maßnahmen
- Dokumentation
- Monitoring

I. Anforderungen – Verarbeitungsverzeichnis

- Jeder Verantwortliche und jeder Auftragsverarbeiter [neu!] führen ein Verzeichnis aller Verarbeitungstätigkeiten (Art. 30 DSGVO).
- Nicht wenn weniger als 250 Mitarbeiter und keine besonderen Risiken für Betroffene

Notwendige Maßnahmen:

- Ermitteln und Dokumentieren aller Verarbeitungen / Data-Mapping
- Prozess für Aktualisierungen und Anpassungen aufsetzen

I. Anforderungen – Datenschutz-Folgenabschätzung

- Bei voraussichtlich hohem Risiko für Rechte und Freiheit Betroffener muss Folgenabschätzung erfolgen.
- Ggf. Meldung an Behörde erforderlich.

Notwendige Maßnahmen:

- Risiko-Analyse durchführen
- Klassifizieren des Risikos („High Risk“)
- Risikovermeidungsmaßnahmen
- Bei verbleibenden Risiken: Meldung an Aufsichtsbehörde

I. Anforderungen – Technikgestaltung/Voreinstellungen

Technische und organisatorische Maßnahmen müssen getroffen werden, dass

- Verarbeitungsprozesse datenschutzfreundlich gestaltet werden (Technikgestaltung / „*Privacy by Design*“) und
- durch Voreinstellungen standardmäßig nur die erforderlichen Daten verarbeitet werden (Voreinstellungen / „*Privacy by Default*“)

I. Anforderungen – Datenschutz Organisation 1/2

- Datenschutzbeauftragten („DPO“) benennen
  - intern oder extern?
  - konzernweit oder lokalen Datenschutzbeauftragten?
- „Datenschutz-Betreuer“ in einzelnen Geschäfts-bereichen?
- Prozesse definieren, wann DPO wie eingebunden wird
- Monitoring und Audits implementieren
- Koordination mit Compliance / Compliance Officer

I. Anforderungen – Datenschutz Organisation 2/2

Datenschutzorganisation mit bekannten Management-Methoden, z. B. PDCA:

Planung und Konzeption / Risikoanalyse

- Umstände, Art, Umfang und Zweck der Verarbeitung
- Wahrscheinlichkeiten
- Risiken für Betroffene

Umsetzung

- Technische und organisatorische Maßnahmen
- Datenschutz-richtlinien /-vorkehrungen
- Nachweise

Erfolgskontrolle und Monitoring

- Laufende Überprüfung der Maßnahmen

Optimierung und Verbesserung

- Aktualisierung der Maßnahmen

I. Anforderungen – Datenschutzklima / interne Kommunikation

Datenschutz muss nach Willen der DSGVO Teil der Unternehmenskultur werden

Maßnahmen:

- Management-Commitment ist erforderlich („*Tone at the top*“ und „*walk the talk*“)
- Trainings
  - Trainings nach Risikobereich abstufen
  - wiederkehrende Trainings implementieren
- Mitarbeitererklärungen zu Datengeheimnis

I. Anforderungen - Löschkonzept

- Unternehmen benötigen ein Löschkonzept: Welche Daten werden wie lange aufgehoben?
- Betroffene müssen über Zeiträume bzw. Bestimmungskriterien informiert werden

Notwendige Maßnahmen:

- Erstellung Löschkonzept, ggf. auf Basis des Verarbeitungsverzeichnisses
- Berücksichtigung etwaiger Aufbewahrungsfristen
- Umsetzung: Implementierung von Löschroutinen

I. Anforderungen - Datensicherheit

- Datensicherheit als Grundprinzip [Art. 5 Abs. 1 f)]:

  Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

- Unternehmen müssen unter Berücksichtigung der Risiken und Kosten geeignete Sicherheitsmaßnahmen treffen (Art 32 Abs. 1).
- Verhaltensregeln (Art. 40) oder Zertifizierungen (Art. 42) geben Orientierung

I. Anforderungen – Data Breach Notification

Bei Verletzung des Schutzes personenbezogener Daten:

- Meldung an Behörde unverzüglich, nicht später als 72 Stunden, es sei denn voraussichtlich kein Risiko;
- bei „hohem Risiko für Rechte und Freiheiten“ unverzüglich Benachrichtigung an Betroffene

Notwendige Maßnahmen:

- Risikoanalyse
- Verantwortlichkeiten und Prozesse definieren
- Technische und organisatorische Maßnahmen zur Risikominimierung

I. Anforderungen - Vertragsmanagement

Verträge sollten überprüft werden, ob diese im Einklang mit der DSGVO stehen, insbesondere bei

- konzerninternem Datentransfer,
- Auftragsdatenverarbeitung (Art. 28, 29 DSGVO),
- internationalem Datentransfer (Art. 44 ff DSGVO) und
- gemeinsamer Datenverantwortlichkeit (Art. 26 DSGVO).

Wichtige generelle Punkte u.a.:

- Rechtsgrundlage für Übermittlung
- „Accountability“ und Dokumentation
- Haftungsfragen

I. Anforderungen - Einwilligungsmanagement

- Hohen Anforderungen und bisherige Einwilligungen sind ggf. an neuen Erlaubnistatbeständen auszurichten (u.a. Kopplungsverbot, Zweckänderung)
- Beweislast liegt bei Unternehmen
  - doppeltes Opt-In
  - elektronische Erklärung
  - schriftliche Bestätigung mündlicher Erklärungen

Notwendige Maßnahmen

- Inhaltliche Überprüfung
- Dokumentation
- Widerrufsmanagement – Prozesse definieren

I. Anforderungen – Transparenz / Betroffenenrechte

- Umfassende Informationspflichten, zu erfüllen in verständlicher, leicht zugänglicher Form
- Betroffenenrechte müssen als Prozess abgebildet und dokumentiert werden:
  - Auskunftsrecht (Art. 15)
  - Recht auf Berichtigung (Art. 16)
  - Recht auf Löschung / auf „Vergessenwerden“ (Art.17)
  - Recht auf Einschränkung der Verarbeitung (Art. 18)
  - Mitteilungspflichten bei Berichtigung / Löschung etc. (Art. 19)
  - Recht auf Datenportabilität (Art. 20)
  - Widerspruchsrecht (Art. 21)

I. Anforderungen – Internationaler Datentransfer

Jeder Datentransfer außerhalb des EWR („Drittstaatentransfer“) erfordert das Sicherstellen eines angemessenen Schutzniveaus (Art. 44 ff.)

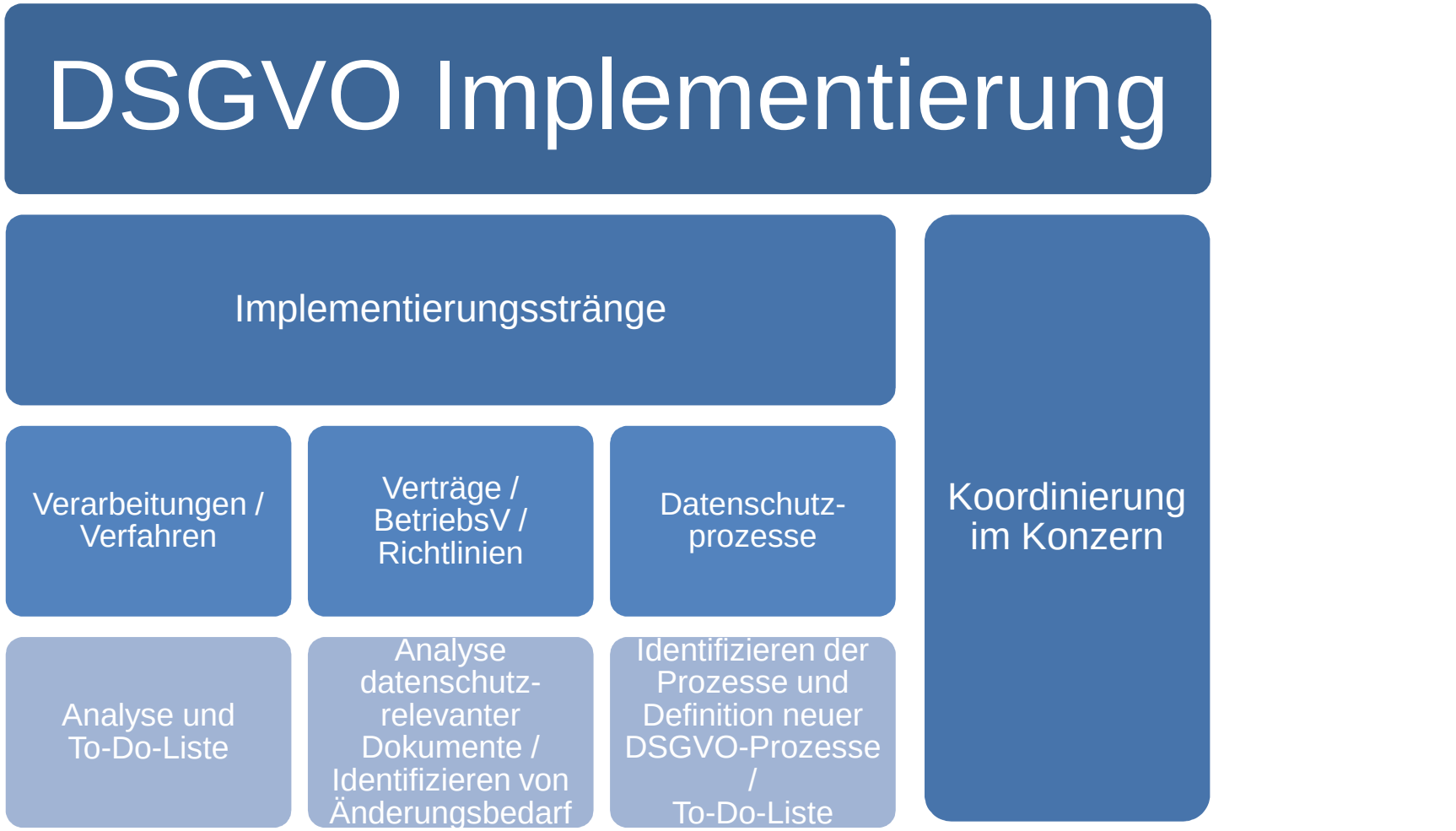
Notwendige Maßnahmen

- Analyse der Datenflüsse mit internationalem Bezug
- Welche Sicherungsmechanismen werden derzeit genutzt?
- Besteht Anpassungsbedarf?

Implementierung

BEITEN BURKHARDT

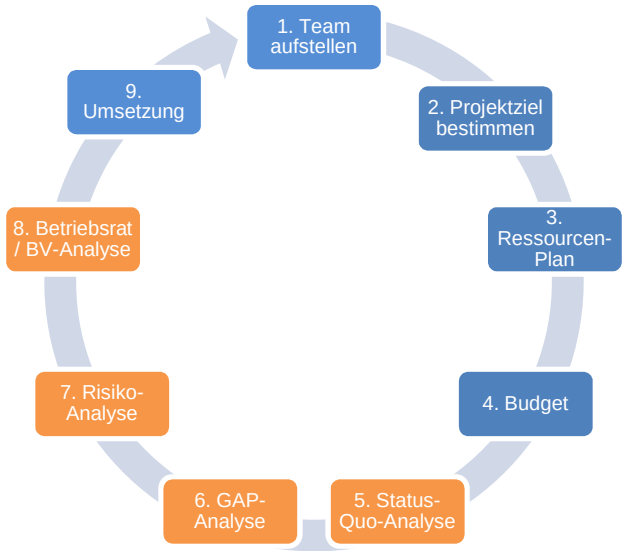
II. Implementierung – Überblick I



II. Implementierung – Überblick II

II. Implementierung – Team aufstellen

- Verfügbare Ressourcen?
- Zusammensetzung
  - IT
  - HR
  - Legal
  - Compliance
  - Management?
- Projektmanagement / Projektleiter



BEITEN BURKHARDT

II. Implementierung – Projektziele

- Projektplan: Konkret und spezifisch
- Abstimmung mit Management
- Planänderungen: Abstimmungsmechanismen wegen Zeit und Budget

BEITEN BURKHARDT

II. Implementierung – Ressourcenplanung

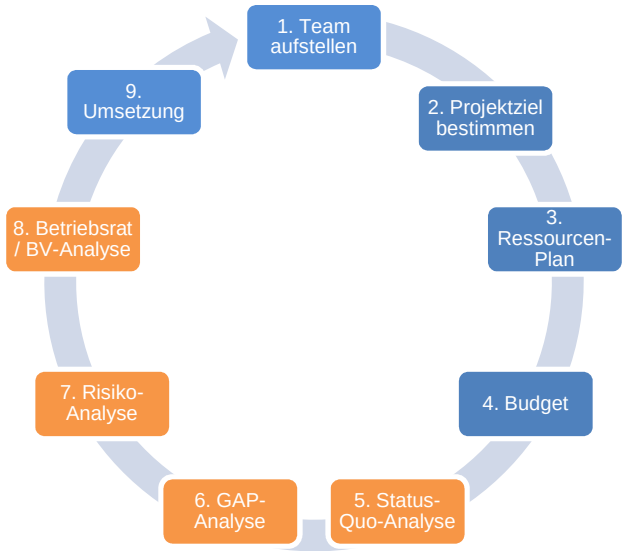
- notwendige Ressourcen bestimmen
- Prozesse und Strukturen analysieren

BEITEN BURKHARDT

II. Implementierung – Budget-Planung

- Vorher klären!
- Softwarekosten
- externe Kosten
- interne Kosten

- Bußgeldrisiko
- Schadensersatzrisiko
- Reputationsschadenrisiko



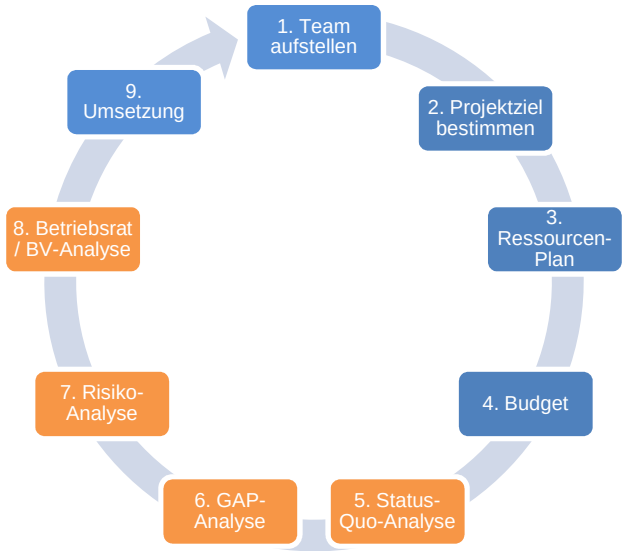
BEITEN BURKHARDT

II. Implementierung – Status-Quo-Analyse

Alle existierenden Datenverarbeitungsaktivitäten im Unternehmen abbilden und dazu alle relevanten

- Geschäftseinheiten
- Betroffenengruppen
- Empfänger

identifizieren.



BEITEN BURKHARDT

II. Implementierung – GAP-Analyse

- Status Quo mit DSGVO-Anforderungen vergleichen
- Anpassungsbedarf identifizieren
- bestehende Strukturen berücksichtigen und einbinden
- Datenflüsse designen

BEITEN BURKHARDT

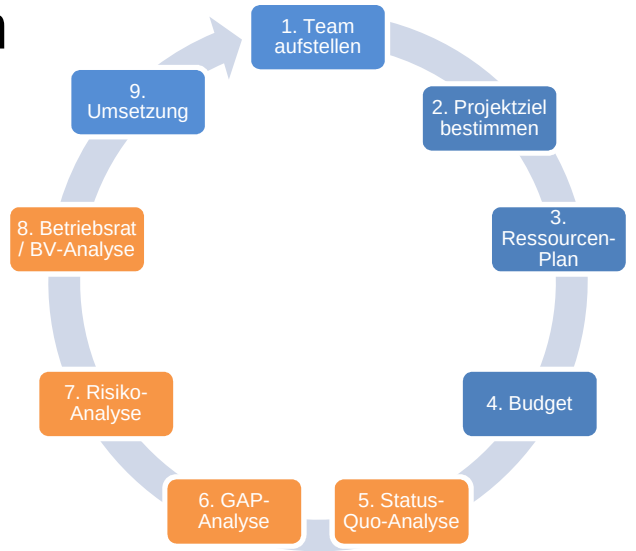
II. Implementierung – Risiko-Analyse

- Risiken identifizieren
- Risikoplan erstellen und Risiken klassifizieren
- Risikominderungsmaßnahmen bestimmen

BEITEN BURKHARDT

II. Implementierung – Betriebsrat / andere Stakeholder einbinden

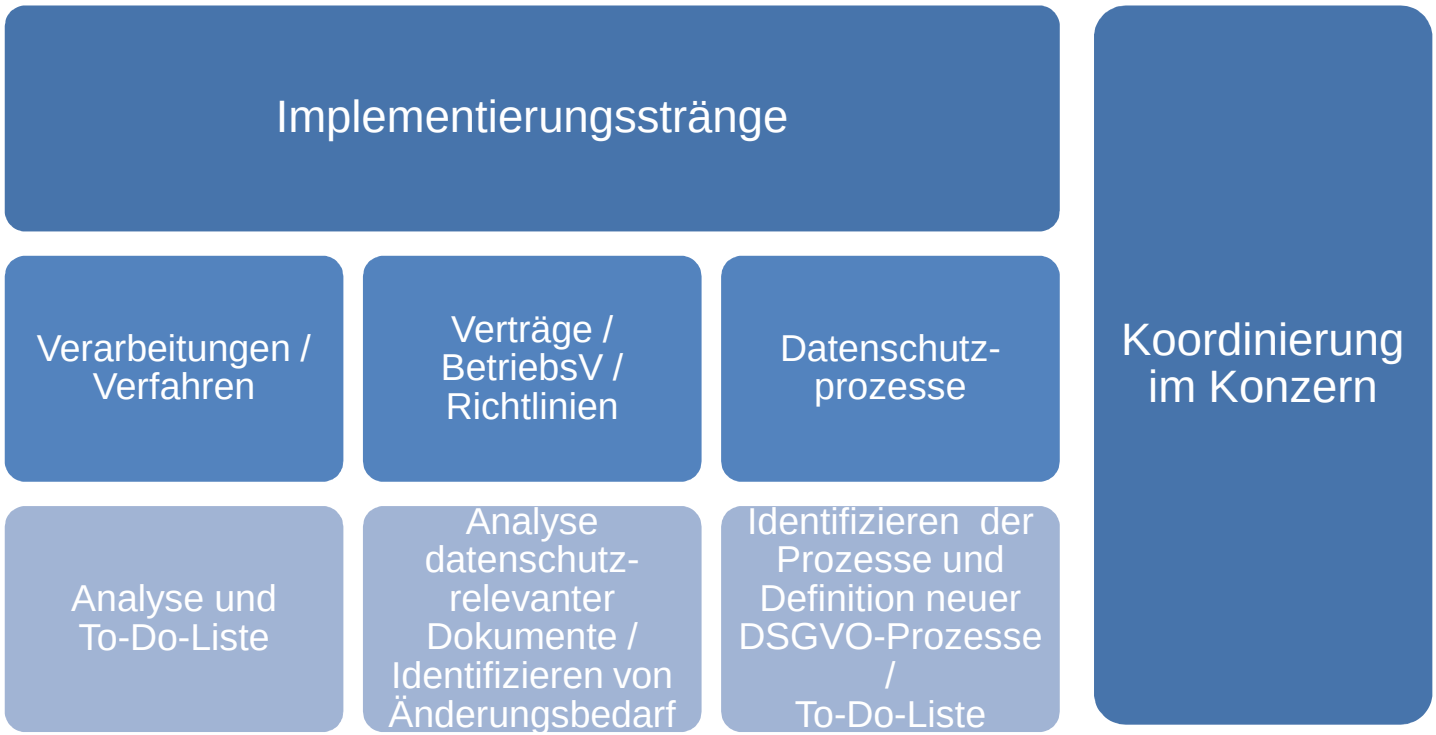
- Betriebsrat hat auch ein Mandat für Datenschutz
- Betriebsvereinbarung müssen vielleicht angepasst werden
- Datenschutzbeauftragter sollte möglichst früh in das Projekt eingebunden werden



Strategie / Roadmap

BEITEN BURKHARDT

DSGVO Implementierung



BEITEN BURKHARDT

III. Strategie / Roadmap

- Priorität sollte auf Verantwortlichkeit, also Erfassung und Dokumentation der Verfahren liegen.
- Leiten Sie daraus die anderen Analysen / Anforderungen ab.
- Umsetzungsbreite und -tiefe: Gewichten Sie nach Risiken.
- Nutzen Sie die Gelegenheit, um Ihre Datenflüsse neu zu ordnen / optimieren.
- Planen Sie ausreichend Zeit für Verhandlungen (BR, Verträge) ein.

ASAP

bis Herbst 2017

25. Mai 2018: Noch 479 Tage…

Sprechen Sie uns an.

BEITEN BURKHARDT

Dr. Axel von Walter

Partner | Rechtsanwalt | Fachanwalt für Urheber- und Medienrecht | Fachanwalt für Informationstechnologierecht
BEITEN BURKHARDT | Ganghoferstraße 33 | 80339 München
Praxisgruppe – IT/IP/Medien
Telefon: +49 89 35065-1321
E-Mail: Axel.Walter@bblaw.com

Axel von Walter ist Partner bei BEITEN BURKHARDT in München und Mitglied der Praxisgruppe IT/IP/Medien. Sein Tätigkeitsbereich umfasst das gesamte Medien- und Informationsrecht, das Recht der Informationstechnologie (einschließlich des Telekommunikations- und Datenschutzrechts) sowie das Wettbewerbsrecht. Im Bereich Datenschutz und Compliance berät er nationale und internationale Mandanten und vertritt diese auch in gerichtlichen Auseinandersetzungen und gegenüber Aufsichtsbehörden.

Axel von Walter studierte Rechtswissenschaften an der Universität München und wurde im Jahr 2004 zur Anwaltschaft zugelassen. Seine Dissertation unter Betreuung von Prof. Dr. Helmut Köhler wurde 2007 mit dem Fakultätspreis der Universität München ausgezeichnet. Vor seinem Einstieg als Partner bei BEITEN BURKHARDT war Axel von Walter für andere international ausgerichtete Kanzleien in München und London im Bereich IP/IT, Medien- und Datenschutzrecht tätig. Axel von Walter ist Lehrbeauftragter für Medien- und Informationsrecht an der juristischen Fakultät der Ludwig-Maximilians-Universität München.

BEITEN BURKHARDT

Über BEITEN BURKHARDT

BEITEN BURKHARDT

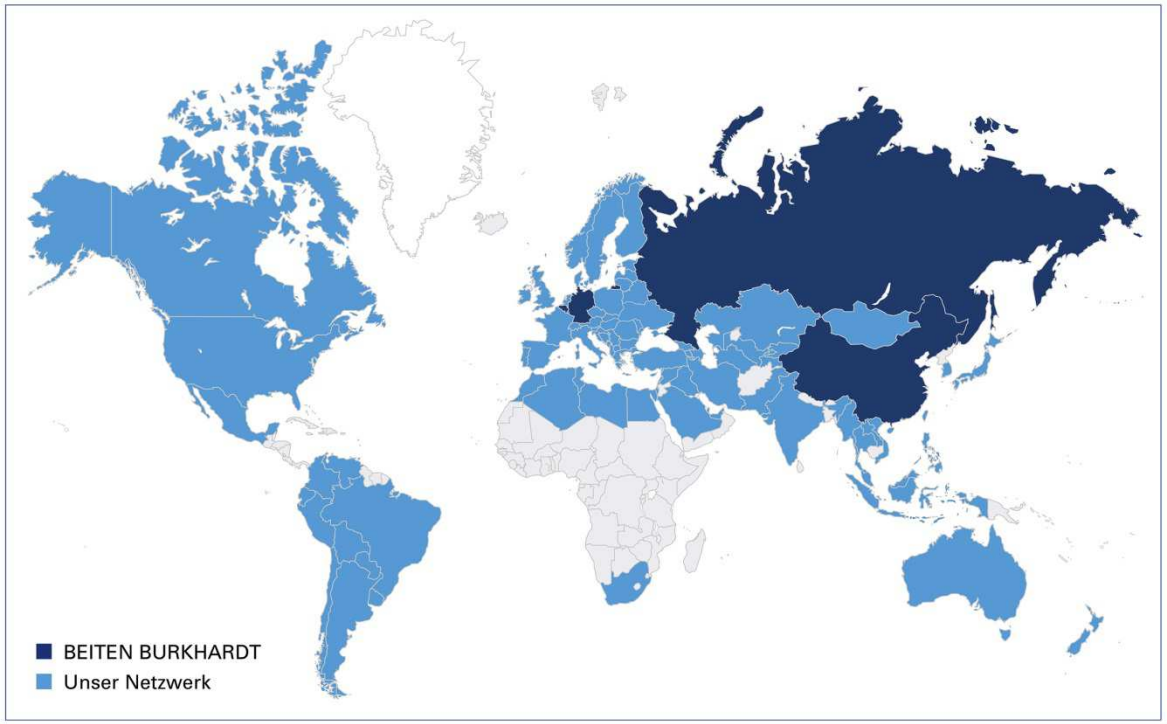
BEITEN BURKHARDT auf einen Blick

BEITEN BURKHARDT ist eine internationale unabhängige Wirtschaftskanzlei.

Gegründet	1990 in München
Berufsträger weltweit	275
in Deutschland	243
im Ausland	32
Standorte	Beijing, Berlin, Brüssel, Düsseldorf, Frankfurt am Main, Moskau, München, St. Petersburg

BEITEN BURKHARDT

Unser Internationales Netzwerk



BEITEN BURKHARDT

Unsere deutschen und internationalen Standorte

BEITEN BURKHARDT

Wo wir sind

Beijing
BEITEN BURKHARDT
Suite 3130, 31st Floor
South Office Tower
Beijing Kerry Centre
1 Guang Hua Road
Chao Yang District
100020 Beijing
China
Tel.: +86 10 85298110
Fax: +86 10 85298123
E-Mail: bblaw-beijing@bblaw.com

Berlin
BEITEN BURKHARDT
Kurfürstenstraße 72 – 74
10787 Berlin
Tel.: +49 30 26471-0
Fax: +49 30 26471-123
E-Mail: bblaw-berlin@bblaw.com

Brüssel
BEITEN BURKHARDT
Avenue Louise 489
1050 Brüssel
Belgien
Tel.: +32 2 6390000
Fax: +32 2 7322353
E-Mail: bblaw-bruessel@bblaw.com

Düsseldorf
BEITEN BURKHARDT
Cecilienallee 7
40474 Düsseldorf
Tel.: +49 211 518989-0
Fax: +49 211 518989-29
E-Mail: bblaw-duesseldorf@bblaw.com

Frankfurt
BEITEN BURKHARDT
Mainzer Landstraße 36
60325 Frankfurt am Main
Tel.: +49 69 756095-0
Fax: +49 69 756095-512
E-Mail: bblaw-frankfurt@bblaw.com

München
BEITEN BURKHARDT
Ganghoferstraße 33
80339 München
Tel.: +49 89 35065-0
Fax: +49 89 35065-123
E-Mail: bblaw-muenchen@bblaw.com

Moskau
BEITEN BURKHARDT
Turchaninov Per. 6/2
119034 Moskau
Russland
Tel.: +7 495 2329635
Fax: +7 495 2329633
E-Mail: bblaw-moskau@bblaw.com

St. Petersburg
BEITEN BURKHARDT
Marata Str. 47-49, Lit. A, office 402
191002 St. Petersburg
Russland
Tel.: +7 812 4496000
Fax: +7 812 4496001
E-Mail: bblaw-stpetersburg@bblaw.com

BEITEN BURKHARDT

WWW.BEITENBURKHARDT.COM

Beijing • Berlin • Brüssel • Düsseldorf • Frankfurt am Main • Moskau • München • St. Petersburg

BEITEN BURKHARDT