

KP&Co.

Datenschutzmanagement

WER SCHÜTZT KLEIN- UND MITTELBETRIEBE VOR DEM DATENSCHUTZ?

DATENSCHUTZ IM MITTELSTAND:

SO WENIG BÜROKRATIE WIE MÖGLICH, ABER SO VIEL WIE NOTWENDIG!

Warum ist Datenschutz plötzlich so wichtig?

Einheitliches Europäisches Recht durch Erlass einer Verordnung

Umsetzungsfrist endet am 24.05.2018

Art.83DSGVO: „*Abschreckende Geldbußen*“:
20 Millionen / 4% des weltweiten Umsatzes

Abmahnung durch Wettbewerber

Künftig nicht nur Schadensersatz, sondern „Schmerzensgeld“

Gerichtsstand beim Betroffenen!

WORÜBER WIR REDEN

Personenbezogene Daten:

„Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (...) beziehen“

(Auszug aus Art. 4 Nr. 1 DSGVO)

- Natürliche Person: keine Daten, die ausschließlich juristische Personen betreffen
- Zuordenbar: z.B. Personalnummer, KFZ-Zeichen, Koordinaten, Fingerabdruck, IP-Adresse (EuGH –Breyer/Deutschland)
- Weitere Beispiele: E-Mail-Adresse, Privatanschrift, Telefonnummern, Urlaubsantrag, Geburtsdatum, Namen, Benutzungszeiten einer Maschine

KP&Co.

Datenschutzmanagement

WORÜBER WIR REDEN

Verarbeiten:

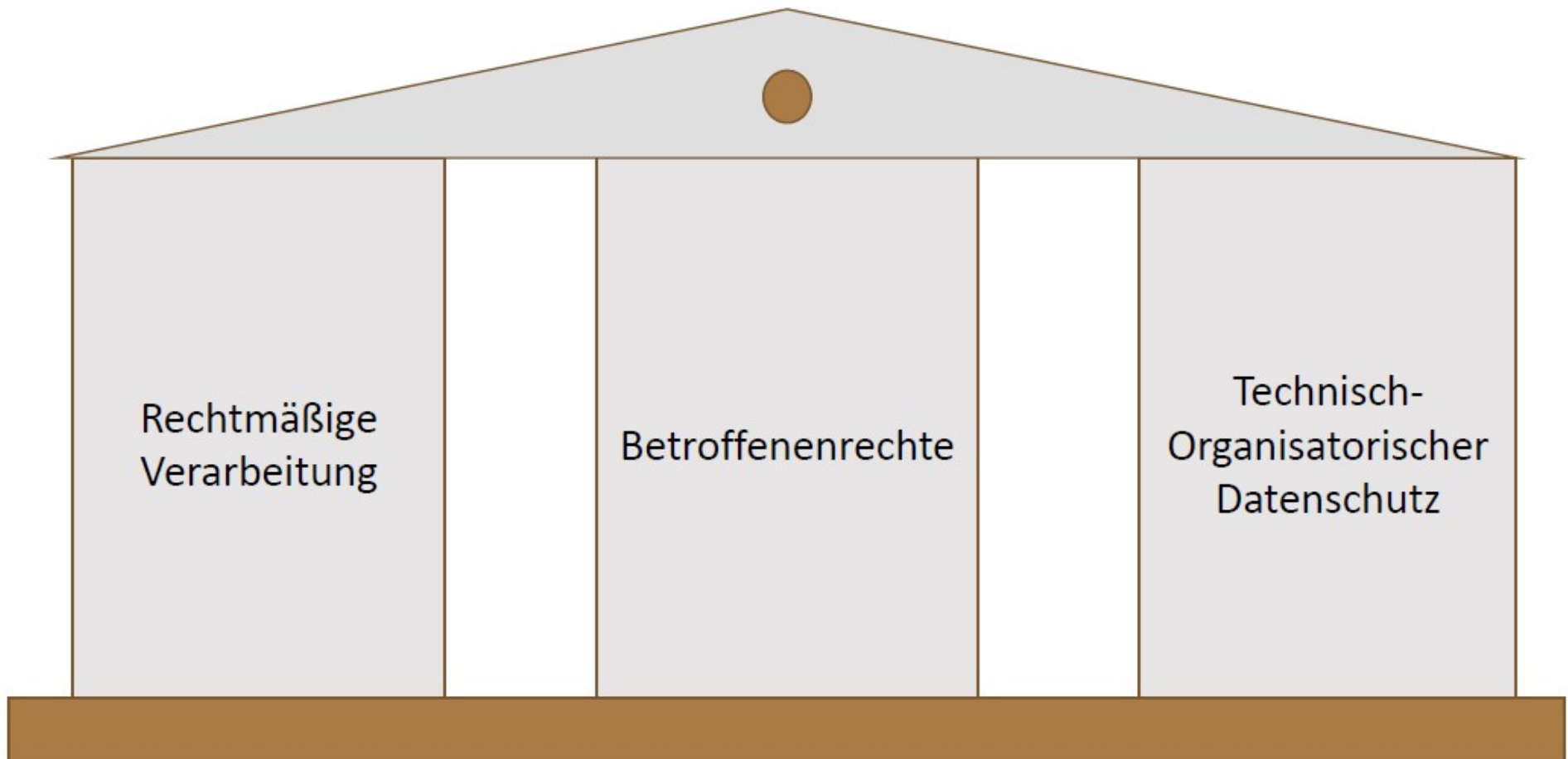
Jeder „Vorgang (...) im Zusammenhang mit personenbezogenen Daten (...)“
(Auszug aus Art. 4 Nr.2 DSGVO)

- **Erfassen**, z.B. Kundendaten beim Termin
- **Speichern**, z.B. von Kundendaten im System
- **Veränderung** z.B. des Familienstands in der Personalakte
- **Auslesen und Abfragen**, z.B. für Ihren Newsletter
- **Verwendung**, z.B. für eine Geschäfts-E-Mail
- **Übermittlung**, z. B. an die Muttergesellschaft
- **Verbreitung** bzw. **Bereitstellung**, z.B. im Internet
- **Abgleich** und **Verknüpfung**, z.B. zur Aufdeckung von Straftaten
- **Einschränkung** und **Löschen**, z. B. bei ausgeschiedenen Mitarbeitern
- **Vernichtung**, z.B. von Akten nach Ablauf von Aufbewahrungsfristen

KP&Co.

Datenschutzmanagement

ÜBERSICHT: DIE WICHTIGSTEN ANFORDERUNGEN



RECHTMÄßIGKEIT DER VERARBEITUNG

Die Verarbeitung von personenbezogenen Daten
ist grundsätzlich verboten!

Wann ist Datenverarbeitung ausnahmsweise erlaubt?

- Einwilligung
- zur Erfüllung eines Vertrags
- zur Erfüllung einer Rechtspflicht
- zur Wahrung berechtigter Interessen sofern
nicht die Interessen des Betroffenen überwiegen

Aber nur, wenn
ERFORDERLICH

KP&Co.

Datenschutzmanagement

RECHTMÄßIGKEIT DER VERARBEITUNG (2)

Sensible Daten

- Ethnie, Religion, sexuelle Orientierung, Politik, Gesundheit, ...
- Restriktivere Ausnahmen:
 - Rechte und Pflichten nach dem Arbeits- und Sozialrecht
 - medizinische Diagnostik
 - Beurteilung der Arbeitsfähigkeit



Sind besonders gut vor Missbrauch und Verlust zu schützen!

Zweckbindung der Daten

- Daten dürfen nur für eindeutige und legitime Zwecke verarbeitet werden.
- Für Zweckänderung neue Erlaubnisnorm nötig
- **Beispiel:** Erhebung für Praktikum, spätere Verwendung für Werbung
- **Merke: der Zweck muss fest definiert und dokumentiert sein!**

KP&Co.

Datenschutzmanagement

RECHTMÄßIGKEIT DER VERARBEITUNG (3)

Grundsatz der Datenminimierung

- Erheben Sie so wenige personenbezogene Daten, wie möglich!
- **Beispiel:** Parteizugehörigkeit eines Arbeitnehmers
- Richten Sie Ihre Organisation entsprechend ein:
 - Z.B. keine personenbezogenen Daten ausdrucken, wenn vermeidbar
 - Z.B. Pseudonymisierung oder Anonymisierung der Daten

Grundsatz der Richtigkeit

- Daten müssen richtig und auf dem neusten Stand sein
- Angemessene Maßnahmen, dies zu gewährleisten

KP&Co.

Datenschutzmanagement

RECHTMÄßIGKEIT DER VERARBEITUNG (4)

Grundsatz der Transparenz

- Gedanke: Ohne Transparenz liefere der Datenschutz weitgehend leer
- Verarbeitung muss für die betroffene Person
 - erkennbar gemacht werden,
 - sie muss über Risiken, Vorschriften und Rechte informiert werden
 - und die Informationen müssen leicht verständlich sein

Grundsatz der Speicherbegrenzung

- Daten dürfen nur so lange aufgehoben werden, wie für den Zweck erforderlich!
- Unternehmen müssen ein System für Löschroutinen aufsetzen
- Große Herausforderung in der Praxis!

KP&Co.

Datenschutzmanagement

RECHTMÄßIGKEIT DER VERARBEITUNG (5)

Grundsätze der Integrität und Vertraulichkeit

- Daten sind durch technische und organisatorische Maßnahmen vor Gefahren zu schützen.
- **Beispiele** für Gefahren:
 - Manipulation durch natürliche Person
 - USB-Stick verloren!
 - Feuer, Blitzschlag etc.

KP&Co.

Datenschutzmanagement

BETROFFENENRECHTE

Informationspflichten (Transparenz)

- Umfangreiche Informationspflicht!
- Art. 13 DSGVO: bei „Erheben“ sowie bei jeder Zweckänderung
- Enorme praktische Bedeutung: Bewerberportale, Vertragsverhandlung mit Lieferanten, Entgegennahme Visitenkarte, Erhalt von Geschäfts-E-Mails, Arbeitsvertragsschluss, Internetrecherche

Auskunftsrechte (Transparenz)

- Auskunftsrecht, ob Daten verarbeitet werden
- Falls ja: Details zu Zwecken, Kategorien, geplante Speicherdauer, etc.

KP&Co.

Datenschutzmanagement

BETROFFENENRECHTE (2)

Recht auf Berichtigung (Richtigkeit)

- Betroffener kann Berichtigung von unrichtigen Daten verlangen

Recht auf Vergessenwerden (Speicherbegrenzung)

- Z.B. wenn nicht mehr „erforderlich“
- Z.B. wenn Einwilligung widerrufen
- Hohes Störpotential für Querulanten!

Recht auf Einschränkung (Speicherbegrenzung/Richtigkeit)

- „Kleiner Bruder“ der Löschung
- Z.B. wenn Richtigkeit bestritten wird
- Nutzbarkeit der Daten dann erheblich beschränkt

KP&Co.

Datenschutzmanagement

BETROFFENENRECHTE (3)

Recht auf Datenübertragbarkeit

- Beruht Datenerhebung auf Einwilligung oder Vertrag, kann Betroffener Bereitstellung z.B. auf USB Stick verlangen.
- Z.B. Beraterverträge, Ärzte, Personaldaten ausscheidender Mitarbeiter (?),

KP&Co.

Datenschutzmanagement

DATENSICHERHEIT

TOMs – Technisch-Organisatorische Maßnahmen

- Sicherung des Zutritts, des Zugangs und des Zugriffs
- Organisatorische Trennung nach Zweck
- Weitergabekontrolle durch Verschlüsselung, Firewall etc.
- Eingabekontrolle durch Protokollierung von Nutzung
- Auftragskontrolle: Kontrolle etwaiger Auftragsdatenverarbeiter
- Verfügbarkeitskontrolle: Schutz vor Beschädigung und Zerstörung

Datenschutzmanagement

DATENSICHERHEIT: RISIKOBASIERTER ANSATZ

Beispiel Risiko-Matrix mit vier Stufen

4 Maximal	4	8	12	16
3 Signifikant	3	6	9	12
2 Eingeschränkt	2	4	6	8
1 Vernachlässigbar	1	2	3	4
	1 Vernachlässigbar	2 Eingeschränkt	3 Signifikant	4 Maximal

Quelle: Risk Assessment & Datenschutz-Folgenabschätzung, Bitkom e.V. 2017

SOFORTMASSNAHMEN

1. Datenschutzbeauftragten bestellen ?
2. Verzeichnis der Verarbeitungstätigkeiten erstellen
3. Auftragsverarbeiter verpflichten
4. Datensicherheit überprüfen
5. Rechenschaftspflicht sicherstellen
6. Ihre Website datenschutzrechtlich gestalten
7. Datenschutz-Management-System aufbauen 

KP&Co.

Datenschutzmanagement

1.

DATENSCHUTZBEAUFTRAGTER: BESTELLEN?

- Mind. 10 Personen verarbeiten personenbezogene Daten
- Wenn nein: ist Datenverarbeitung Ihre Kerntätigkeit und macht dies die Überwachung erforderlich?



Nicht vergessen: Kontaktdaten des DSB sind an die Aufsichtsbehörde zu melden und zu veröffentlichen!

2.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

- **Verfahrensverzeichnis** = Verzeichnis aller Verarbeitungsvorgänge im Unternehmen
- „**Verarbeitung**“ z.B. Finanzbuchhaltung, Reiseplanung, Entgeltabrechnung, Arbeitszeiterfassung, Personalaktenführung, Newsletter, E-Mail-System
- Im Verzeichnis: Angaben zu Zweck, Grundlage, Betroffenen, Empfänger, Drittstaatentransfer, Speicherdauer...
- Falls nicht vorhanden, unbedingt hiermit anfangen!

3.

AUFTRAGSVERARBEITER

- Dienstleister, die Daten auf Ihre Weisung hin verarbeiten
- DSGVO: „Auftragsverarbeitung“, Zweck und Mittel vorgegeben
- Z.B. Rechenzentren, Datev, Cloud-Anbieter
- Vorsicht bei Auswahl und Kontrolle!
- Vertrag sauber gestalten!
- Auftragsverarbeiter bekommen durch DSGVO zahlreiche neue Pflichten!

4.

DATENSICHERHEIT ÜBERPRÜFEN!

- Zuerst: Risiko-Assessment (s.o.)
- Schützen Sie zunächst besonders kritische Daten und arbeiten Sie sich vor!
- Bei besonderen Risiken zudem: **Datenschutz-Folgenabschätzung**
 - Systematische Bewertung der Verarbeitungsvorgänge
 - Ersetzt heutige Vorabkontrolle
 - Konsultation der Behörde bei hohem Risiko
- Aufsichtsbehörden sind in der Pflicht und sollen White-List/Black-List erstellen (steht noch aus!)

KP&Co.

Datenschutzmanagement

DATENSICHERHEIT ÜBERPRÜFEN! (2)

- Achtung: Meldepflicht für Datenschutzverletzungen binnen 72 Stunden
 - Verlorener USB-Stick, Fax oder E-Mail an den falschen Adressaten
 - Anzugeben sind z. B. Vorgang, Kategorien der Daten, Anzahl der Betroffenen, mögliche Folgen, Maßnahmen zur Schadensminimierung
 - Bußgeld: bis 10 Mio. / 2 % des Umsatzes
 - Schulen Sie Ihre Arbeitnehmer, welche Vorfälle unbedingt gemeldet werden müssen
 - Richten Sie ein Warnsystem ein!

5.

RECHENSCHAFTSPFLICHT (ACCOUNTABILITY)!

- Dokumentieren Sie, dass Ihr Unternehmen die DSGVO beachtet in einem Rechenschaftsbericht
- Aufsichtsbehörden werden künftig Vorlage einer entsprechenden Dokumentation verlangen!

6.

IHRE WEBSITE: ALLGEMEINES

- Bisher: § 4 Abs. 3, § 33 BDSG und § 13 Abs. 1 TMG
- Künftig: Art. 13 und 14 DSGVO
- Datenschutzerklärung zwingend (bußgeldbewehrt, abmahnfähig)
- Am besten isoliert von anderen Bedingungen (Impressum / AGB)
- Informationen müssen schon bei Erhebung bereitgestellt werden (aber: Verlinkung zulässig)
- leicht wahrnehmbarer, verständlich und klar nachvollziehbar
- Angepasst auf jeweilige Gestaltung / Datenverarbeitung

KP&Co.

Datenschutzmanagement

IHRE WEBSITE: MINDESTINHALTE

- Speicherdauer oder Kriterien, nach denen sich die Speicherdauer bestimmt
- Benennung der Rechte des Betroffenen auf Zugang, Berichtigung, Sperrung, Löschung, Widerspruch und Datenübertragbarkeit
- Beschwerderecht
- Widerrufsrecht
- Herkunft der Daten, wenn nicht beim Betroffenen erhoben (auch öffentlich zugängliche Quellen)
- Tracking, Profiling (Newsletter, automatisierte Einzelfallentscheidungen)
- Blog mit Kommentarfunktion (Pseudonyme, Abonnement von Kommentaren)
- Weitergabe von Daten an Dritte
 - Dienstleister für Bestellabwicklungen
 - Social-Media-Plugins
 - Online-Bestellformulare (Warenwirtschaftssystem)
 - Bezahldienste
 - Analysedienste (Google Analytics, Piwik, Adobe Analytics etc.)
 - Anzeigen- und Marketingdienste (Google AdSense / AdWords etc.)

KP&Co.

Datenschutzmanagement

IHRE WEBSITE: COOKIES + GOOGLE ANALYTICS

COOKIES

- Bei Verwendung stets Hinweis erforderlich
- Einwilligung je nach Gestaltung fraglich

GOOGLE ANALYTICS

- In jedem Fall gesonderter Hinweis in Datenschutzerklärung erforderlich
- „Untergeschobene“ (stillschweigende) Zustimmung rechtlich problematisch
 - „Durch die Nutzung dieser Website erklären Sie sich mit der Bearbeitung der über Sie erhobenen Daten durch Google in der zuvor beschriebenen Art und Weise und zu dem zuvor benannten Zweck einverstanden.“

SOCIAL MEDIA PLUG-INS

- Verwendung stets fraglich
- EuGH-Urteil zu Facebook

KP&Co.

Datenschutzmanagement

EXKURS: E-PRIVACY VERORDNUNG

- Inkrafttreten voraussichtlich erst 2019
- Ermöglichung der Datenkontrolle durch Bürger
- Adressaten: Webseiten, Plattformen, Werbewirtschaft
- Opt-In: Verbot der Nutzung ohne ausdrückliche Einwilligung
- Steigende Bedeutung von Cookies / Social Media Logins
- VDZ (29.1.2018): Über 30 Prozent Umsatzverlust im digitalen Werbegeschäft für journalistische Medien zu erwarten

KP&Co.

Datenschutzmanagement

7.

DATENSCHUTZ-MANAGEMENT-SYSTEM

Planung

- Zusammenstellung eines Datenschutz-Teams
- Bestandsaufnahme: Datenfluss und Prozesse
- Prüfung Rechtmäßigkeit der Verarbeitung

Durchführung

- Durchführung Risk-Assessment
- Erstellen einer Verarbeitungsübersicht
- Sicherstellung geeigneter Schutzmaßnahmen
- Prozess zur Umsetzung Betroffenenrechte (Löschroutinen, Schulungen, Datenschutzerklärungen)
- Anpassung Verträge Auftragsdatenverarbeitung
- Dokumentation (Rechenschaftspflicht)
- Erstellung Datenschutz-Folgenabschätzung
- Ggf. Bestellung Datenschutzbeauftragter

Follow-up

- Überwachung
- Anpassung bei technischen und organisatorischen Neuerungen
- Neue Rechtslagen

DATENSCHUTZ IM MITTELSTAND:

SO WENIG BÜROKRATIE WIE MÖGLICH, ABER SO VIEL WIE NOTWENDIG!

Wir bieten belastbaren Datenschutz für Klein- und Mittelbetriebe!

Sie möchten belastbaren Datenschutz aufbauen, der alle Pflichten zur DSGVO einhält und sie vor den vielfältigen Risiken schützt?

Unser Konzept:

KP&Co.

Datenschutzmanagement

DATENSCHUTZ LEISTUNGSPAKETE

Externer Datenschutzbeauftragter

- Bereitstellung des Datenschutzbeauftragten (Art 37 DSGVO)
- Übernahme der Pflichten des Datenschutzbeauftragten (Art 39 DSGVO)
- Ansprechpartner für Landesbehörde und internen/externe Betroffene
- Bereitstellung von Handlungsempfehlungen und Muster
- Mitglied/Fortbildungen im GDD e.V.

Dienstleistungen des Datenschutzbeauftragten

- Dokumentation des Datenschutz-Management-Systems
- Unterstützung bei Erstellung von Leitlinien zum Datenschutz (Art 5 DSGVO)
- Beratung mit Vorlagen zur Verpflichtungserklärung der Mitarbeiter (Art 32.4 DSGVO)
- Erstellung/Führung des Verarbeitungsverzeichnisses (Art 30 DSGVO)
- Beratung mit Vorlagen zur Erstellung der Auftragsdatenverarbeitungen (Art 30.2 DSGVO)
- Datenschutzbildung der Mitarbeiter (Art 39.1b DSGVO)
- Unterstützung/Beratung zur Datenschutzfolgenabschätzung
- Unterstützung/Beratung zu Datenschutzerklärungen Kunden, Mitarbeiter und Webseite
- Durchführung der Datenschutz-Audits und Berichterstattung
- Jährlicher Tätigkeitsbericht an die Geschäftsführung

Umsetzungs- Begleitung

- Begleitung bei der Realisierung eines Datenschutz-Compliance-Managementsystems (Art 5.1a DSGVO)
- Lfd. Überprüfung und Anpassung von Formularen und Checklisten
- Aktuelle Informationen zu Gesetzen, Verordnungen und Bestimmungen zum Datenschutz

KP&Co.

Datenschutzmanagement

DATENSCHUTZ LEISTUNGSPAKETE: GEBÜHREN

Externer Datenschutzbeauftragter	Dienstleistungen des Datenschutzbeauftragten	Umsetzungs- Begleitung
Bereitstellung des Datenschutzbeauftragten BASISPAKET (pauschal) NIEDRIGE ANFORDERUNGEN € 150 mtl. Handwerksbetriebe gewerbliche Selbständige Freiberufler MITTLERE ANFORDERUNGEN € 250 mtl. Werkstätten Produktionsbetriebe Handel HÖHERE ANFORDERUNGEN € 350 mtl. größere Betriebe (über 50 MA) Ärzte / Heilberufe Steuerberater / Anwaltskanzleien DATENSCHUTZ-MANAGEMENT-SYSTEM € 25 mtl. Lizenz und Wartung lfd. Führung der Dokumentation	ABRECHNUNG gemäß EINZELAUFTRAG : Zeitgebühr - volle Gebühr € 70 je halbe Stunde, - davon 7/10 bis 10/10 der vollen Gebühr je nach Schwierigkeitsgrad	ABRECHNUNG gemäß EINZELAUFTRAG : Zeitgebühr oder vereinbarte Jahrespauschale