WHITE PAPER

EU DATENSCHUTZ-GRUNDVERORDNUNG – BESTANDSAUFNAHME 2019

.CPC

avocado rechtsanwälte

EU Datenschutz-Grundverordnung – Bestandsaufnahme 2019

Seit Geltung der EU Datenschutz-Grundverordnung (DSGVO) sind viele Unternehmen weiterhin damit beschäftigt, die umfassenden neuen datenschutzrechtlichen Anforderungen umzusetzen. Ein gut aufgestelltes Datenschutz-Management ist für Unternehmen wichtiger denn je – dabei sollten Unternehmen die ersten Erfahrungen mit der DSGVO berücksichtigen.

Die DSGVO hat seit ihrer Geltung am 25. Mai 2018 zu vielen, teilweise skurrilen Missverständnissen geführt. In Medienberichten war zu lesen von Kindergärten, die Erinnerungsfotos schwärzten, Vermietern, die Klingelschilder abmontierten und Kindermalwettbewerben, bei denen die Gewinner nicht festgestellt werden konnte, weil der Veranstalter aus Datenschutzgründen nur die Vornamen der teilnehmenden Kinder notierte. Abseits dieses Medienrummels arbeiten viele Unternehmen weiterhin daran, die umfassenden Anforderungen der DSGVO umzusetzen.

Aus unternehmerischer Perspektive ist es das Ziel eines DSGVO-Umsetzungsprojekts, eine solide Position gegenüber datenschutzrechtlichen Aufsichtsbehörden und Gerichten zu schaffen. Eine 100%-Umsetzung aller Anforderungen ist mittelfristig kaum möglich.

Die DSGVO hat für Unternehmen umfassende neue Pflichten gebracht, welche diese nicht nur einhalten, sondern die Einhaltung unter Umständen auch nachweisen können müssen. Viele Unternehmen befinden sich aktuell noch mitten im Projekt zur Umsetzung der Anforderungen der DSGVO. Entscheidend ist bei der Umsetzung, die Erfahrungen anderer Unternehmen und die tatsächliche Entwicklung der Risiken im Auge zu behalten, um das Projekt bestenfalls auf geänderte oder neue Risiken ausrichten zu können.

BENCHMARK – WO STEHEN DIE ANDEREN?

Aktueller Stand vieler Umsetzungsprojekte

Auch wenn viele deutsche Unternehmen die zweijährige Umsetzungsfrist vor Geltung der DSGVO kaum genutzt haben, haben mittlerweile die meisten Unternehmen ein Projekt zur Umsetzung der Anforderungen der DSGVO durchgeführt oder zumindest begonnen. Dabei haben jedoch nur wenige Unternehmen aktuell bereits eine vollständige Umsetzung aller Anforderungen erreicht. Vielmehr haben die meisten Unternehmen einen risikobasierten Ansatz gewählt und **zunächst die nach außen „sichtbaren" Maßnahmen umgesetzt**, wie beispielsweise die Benennung des Datenschutzbeauftragten, die Erstellung von Datenschutzhinweisen (insbesondere auf der Website) und den Abschluss von Auftragsverarbeitungsverträgen.

Nächste Etappenziele

Nach der Umsetzung der „sichtbaren" Maßnahmen müssen Unternehmen jetzt verstärkt den Fokus auf andere „notwendige" Maßnahmen legen. Das sind solche Maßnahmen, deren Umsetzung von der DSGVO zwingend gefordert wird und deren Fehlen im Fall einer Untersuchung durch eine datenschutzrechtliche Aufsichtsbehörde sicherlich zu Sanktionen führen würde. Als nächste Schritte stehen daher bei vielen Unternehmen insbesondere die folgenden Maßnahmen an:

- Verzeichnis von Verarbeitungstätigkeiten fertigstellen und flankierende Prozesse implementieren (z.B. für neue oder geänderte Verarbeitungen)
- Technische und organisatorische Maßnahmen zur Datensicherheit implementieren
- Prozess zur Datenschutz-Folgenabschätzung implementieren
- Löschkonzept entwerfen und Anforderungen in allen betroffenen IT-Systemen umsetzen
- Prozess zur effizienten und automatisierten Bearbeitung von Betroffenenanfragen implementieren
- Reaktion auf Datenschutzverletzungen festlegen und entsprechende Prozesse im Unternehmen bekannt machen

WELCHE RISIKEN DROHEN TATSÄCHLICH?

Was machen die datenschutzrechtlichen Aufsichtsbehörden?
Nach der großen Panik zur Einführung der DSGVO und den vorhergesagten Millionen- oder gar Milliardenbußgeldern ist es in den ersten Monaten nach Einführung der DSGVO um die datenschutzrechtlichen Aufsichtsbehörden erstaunlich ruhig geblieben. Anfang 2019 gab es in Frankreich ein Bußgeld **in Höhe von 50 Millionen Euro** gegen Google. Das höchste bekannte DSGVO-Bußgeld in Deutschland belief sich auf vergleichsweise niedrige 80.000 Euro. Laut Medienberichten sind die deutschen Datenschutzaufsichtsbehörden in einer Vielzahl an laufenden Ermittlungsverfahren beschäftigt. Die Ermittlungen sind jedoch sehr zeitintensiv und viele datenschutzrechtliche Aufsichtsbehörden sind aktuell (noch) personell stark unterbesetzt.

Bei den bislang bekannt gewordenen Ermittlungsverfahren lag der Fokus der Ermittlung u.a. auf

- Verletzungen der Datensicherheit (beispielsweise durch unzureichende Verschlüsselung),
- **Einhaltung der Transparenzpflichten** der DSGVO, sowie
- Verwendung von rechtswidrigen Werbemails.

Zusätzlich betreiben einige datenschutzrechtliche Aufsichtsbehörden groß angelegte Prüfungen mittels Fragebögen zur Umsetzung der DSGVO, der Datenschutzorganisation oder speziell zur korrekten Gestaltung der Facebook Fanpages.

Nach einer in 2018 erschienen Studie der Allianz summieren sich die Schäden durch Cybervorfälle weltweit auf jährlich 500 Milliarden Euro und gehören damit zu den größten Risiken für Unternehmen.

Sonstige Risiken?
Von der viel beschriebenen Abmahnwelle ist bislang bis auf wenige Ausnahmen nichts zu sehen. Die Zulässigkeit von DSGVO-Abmahnungen wurde dabei von den Gerichten bislang unterschiedlich bewertet. Auch wenn ein Anstieg von Abmahnungen künftig weiterhin möglich bleibt, scheinen DSGVO-Abmahnungen mittelfristig ein vergleichbar geringes Risiko zu sein.

Anders sieht die Situation bei **datenschutzrechtlichen Schadensersatzklagen** aus. Diese könnten durch das neue Musterfeststellungsverfahren und die auf EU-Ebene diskutierte europaweite Sammelklage künftig zu einer ernsten Herausforderung für Unternehmen werden. Unverändert hoch bleiben die Risiken von möglichen **Reputationsschäden** bei datenschutzrechtlichen Verstößen.

ERKENNTNISSE AUS DSGVO-PROJEKTEN

In Anbetracht der immer noch sehr hohen Risiken und den aktuellen Umsetzungsständen in vielen Organisationen, steht eine erfolgreiche und vollumfängliche Implementierung der DSGVO-Anforderungen in vielen Unternehmen nach wie vor auf der Agenda. Damit dies gelingt, lassen sich unserer Erfahrung nach aus bereits durchgeführten DSGVO-Projekten die folgenden Erkenntnisse ableiten:

- Ein DSGVO Umsetzungsprojekt kann nur effektiv sein, wenn es von der Vorstands- bzw. Geschäftsführungsebene mitgetragen wird.
- Die Umsetzung kostet Zeit und Geduld – aber Unternehmen können schnell etwas bewirken und die Umsetzung kontinuierlich vorantreiben.
- Datensicherheit kann nicht nur rein technisch erreicht werden, sondern erfordert Veränderungen in der Ablauf- & Aufbauorganisation.
- Nachhaltige Lösungen erzielen Sie durch eine Bewusstseins- & Verhaltensänderung bei den handelnden Personen.
- Dazu ist eine frühzeitige, aktive Einbindung von Mitarbeitern ratsam, die täglich mit personenbezogenen Daten umgehen und diese verarbeiten.

Mit Blick auf die datenschutzrechtlichen Aufsichtsbehörden gilt:

- Die datenschutzrechtlichen Aufsichtsbehörden belohnen kooperatives Verhalten – ggf. auch mit niedrigeren Bußgeldern.
- Aktuell sind auch die datenschutzrechtlichen Aufsichtsbehörden überfordert – das kann sich durch geplante Personalaufstockungen aber schnell ändern.

ERFOLGREICHE UMSETZUNG ANHAND EINES BEISPIELS

avocado rechtsanwälte und die CPC Unternehmensmanagement AG bieten gemeinsam einen ganzheitlichen, an der Praxis bewährten, Ansatz zur Implementierung der DSGVO-Anforderungen an. So auch bei einem Kunden aus der Finanzbranche.

Ein aus mehreren Konzerngesellschaften bestehender Finanzdienstleister im B2B-Segment setzt sich das Ziel, bis zum Inkrafttreten der DSGVO die wichtigsten Anforderungen (insbesondere mit Außenwirkung) umgesetzt und längerfristige Maßnahmen angestoßen zu haben. avocado rechtsanwälte und die CPC Unternehmensmanagement AG haben dieses Projekt von Anfang an bis zu seinem erfolgreichen Abschluss begleitet:

Analyse
Um zu verstehen welche Auswirkungen die DSGVO auf das Unternehmen hat, führten die Beteiligten zunächst ein Datenschutzaudit durch. Dabei wurden die Anforderungen der DSGVO an der vorhandenen Situation des Unternehmens gespiegelt. Dabei wurden die vorhandene Aufbau und Ablauforganisation, Governancestrukturen (inklusive Richtlinien und Verträge) sowie die vorhandene IT in die Analyse einbezogen. Auch unternehmenskulturelle und mitarbeiterspezifische Faktoren wurden berücksichtigt (z.B. Wie wird das Thema „Datenschutz“ von den Mitarbeitern gesehen? Über welchen Kenntnisstand verfügen sie zum Thema?).

Im Ergebnis erhielt der Kunde eine Darstellung über alle Herausforderungen und den erforderlichen Handlungsbedarf sowie Handlungsempfehlungen zur priorisierten zeitlichen Umsetzung. Die Priorisierung richtete sich nach dem nach außen hin Sichtbarem, dem Notwendigen und dem für das Unternehmen Sinnvollem.

Konzeption und Aufsetzen des Umsetzungsprojektes
Die beschlossenen Maßnahmen wurden in sechs inhaltliche „Workstreams“ eingeteilt, deren Realisierung jeweils von Kundenmitarbeitern besetzt und verantwortet wurden. Die Gesamtleitung des Projektes erfolgte durch eine Doppelspitze aus Kundenprojektleiter und Berater. Die obersten Führungsebenen war durch den Lenkungskreis abgebildet.

Die Umsetzung wurde in wöchentlichen Sprints geplant. So wurde sichergestellt, dass die Veränderung sofort greifbar und sichtbar wurde. Zudem konnten kurzfristige Anforderungen auf diese Weise schnell erfasst, priorisiert und umgesetzt werden.

Nachhaltige Implementierung durch Einbindung der Betroffenen
Veränderte Verfahren und Verhaltensweisen müssen auch wirksam sein. Damit dies gelingt, müssen Menschen in ihrer Organisation das richtige Bewusstsein im Umgang mit Daten besitzen, die neue Verfahrensweisen akzeptieren und in den neuen Prozessen und Verfahren befähigt werden. Dabei haben sich insbesondere die folgenden Strategien bewährt:

---

1. **Datenschutz muss nicht immer kompliziert sein.** Daher erfolgten notwendige Prozessveränderungen anhand bestehender Prozesse und bekannter Abläufe. Diese wurden in Workshops gemeinsam mit den Betroffenen erarbeitet. Das Ergebnis waren schlanke, kunden- und mitarbeiterorientierte Anpassungen, die in datenschutzkonformen Prozessen mündeten und bei den Betroffenen in hohem Maße akzeptiert wurden.

---

2. **Datenschutz lässt sich leicht in die tägliche Arbeit einbinden.** Gemeinsam mit den betroffenen Mitarbeitern wurden Guidelines und Merkhilfen erstellt und Strategien definiert, wie Datenschutzanforderungen leicht in den Arbeitsalltag integriert werden können. Im Ergebnis gewannen die Mitarbeiter an Handlungssicherheit und die Wahrscheinlichkeit für Datenschutzverstöße wurde gesenkt.

---

3. **Datenschutz ist Teamarbeit.** Diese Aktivitäten wurden durch übergeordnete und abteilungsübergreifende Befähigungsmaßnahmen flankiert, in die auch das höhere Management einbezogen wurden. So wurde beispielsweise großflächig kommuniziert, wie die Informationspflichten und Betroffenenrechte über den gesamten Kundenlebenszyklus und über einzelne Abteilungen hinweg umgesetzt werden.

Das Ergebnis aller Aktivitäten war eine termingenaue Umsetzung der wichtigsten Datenschutzanforderungen pünktlich zum Inkrafttreten der DSGVO, die von den betroffenen Mitarbeitern sofort umgesetzt werden konnten.

Eine hohe Akzeptanz der umgesetzten Maßnahmen auf Seiten der Mitarbeiter und Geschäftspartner stellt eine nachhaltige Umsetzung sicher.

ÜBER AVOCADO RECHTSANWÄLTE

avocado rechtsanwälte ist mit über 50 Anwälten und 75 weiteren Mitarbeitern in Berlin, Frankfurt am Main, Hamburg, Köln, München und Brüssel tätig.
Unsere Tätigkeit umfasst die gesamte wirtschaftsrechtliche Beratung mit Schwerpunkten im Arbeitsrecht, Bankrecht, Gesellschaftsrecht, Immobilienrecht, Informationstechnologierecht einschl. Datenschutzrecht, Öffentlichen Recht und in der Prozessführung.
Wir beraten und vertreten in den Bereichen Informationstechnologie und Datenschutz seit langem eine Vielzahl von Unternehmen aus allen Branchen, vom Mittelstand bis hin zu internationalen Konzernunternehmen.
Zu den zahlreichen von uns betreuten Mandaten gehören insbesondere

- klassische IT-Projekte (Einführung neuer IT-Systeme bzw. Produkte, SAP-Projekte, ERP-Systeme, E-Commerce-Projekte, SaaS, Hosting / Rechenzentren, Supportvereinbarungen, Kooperationsvereinbarungen, Lizenzverträge etc.),
- IT-Outsourcing- und Business Process Outsourcing Projekte (Rahmenverträge, Service Level Agreements usw.), Cloud Computing,
- datenschutz- und datensicherheitsrechtliche Fragestellungen (Umsetzung der DSGVO in Unternehmen, Auftragsverarbeitung, internationale Datentransfers, Datenschutzaudits, produktbezogene Datenschutzberatung z. B. in den Bereichen Payment Services, Mobile Devices, Social Media, Smart-Metering / Smart-Grid etc.),
- die außergerichtliche und gerichtliche Konfliktlösung sowie
- die Unterstützung im Umgang mit datenschutzrechtlichen Aufsichtsbehörden, z. B. bei Auskunftsersuchen, Kontrollen oder Bußgeldverfahren.

avocado
rechtsanwälte

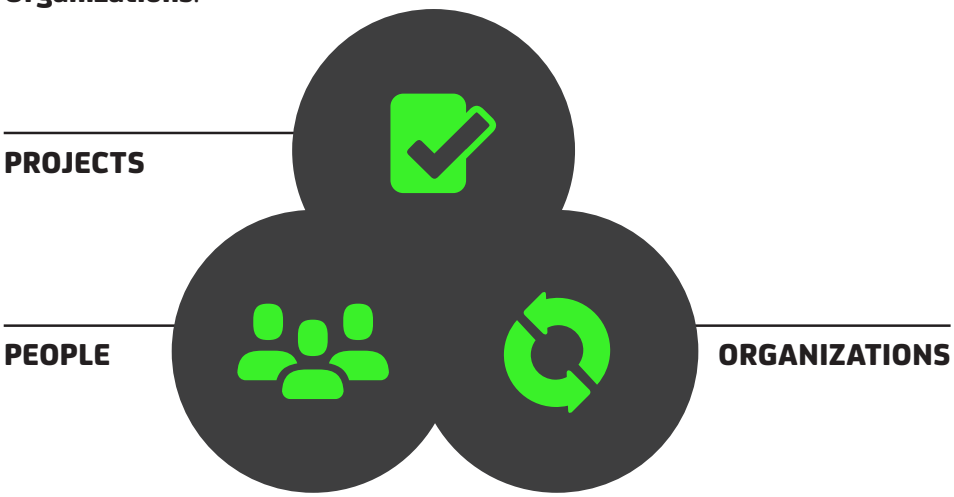
avocado rechtsanwälte
Nextower
Thurn-und-Taxis-Platz 6
60313 Frankfurt am Main
T +49 69 9133010
F +49 69 91330119
www.avocado.de

JAN PETER VOSS
PARTNER
T +49 69 913 30 11 32
j.voss@avocado.de

PROF. DR. THOMAS WILMER
COUNSEL
T +49 69 913 30 11 32
t.wilmer@avocado.de

ÜBER CPC

CPC ist eine führende Change Management-Beratung in Deutschland. Wir sind der verlässliche Partner nachhaltiger Veränderungen. Diese Veränderungen erzielen wir durch eine ganzheitliche, kundenbezogene Vorgehensweise mit den drei Kernkompetenzen **People**, **Projects** und **Organizations**.



Vor mehr als 25 Jahren startete CPC ihre Beratungstätigkeit mit dem Fokus auf Reorganisation im Mittelstand. Heute sind wir ein führender Change-Partner für große Unternehmen. Die Erfahrungen unserer 100 Berater zeigen: Standardlösungen führen nicht zum Ziel, jede Veränderung ist einzigartig. In mehr als 1500 nationalen und internationalen Projekten haben wir einen Methoden- und Formatbaukasten entwickelt und gelernt, diese Werkzeuge bei unternehmerischen Veränderungen gekonnt einzusetzen und präzise, individuelle Lösungen zu schaffen.
Seit Januar 2018 ist CPC als **„Hidden Champion für Change Management und Umsetzung“** ausgezeichnet.

CPC Unternehmensmanagement AG
The Squaire 11
Am Flughafen
60549 Frankfurt am Main
T +49-69-56 03 03 03
F +49-69-56 03 03 05
contact@cpc-ag.de
www.cpc-ag.de

.CPC

CLEMENS HEISINGER
PARTNER
M +49-171-442 35 04
clemens.heisinger@cpc-ag.de

DIRK THATER
BERATER
M +49-160-97 43 61 86
dirk.thater@cpc-ag.de