Warth & Klein Grant Thornton

An instinct for growth™

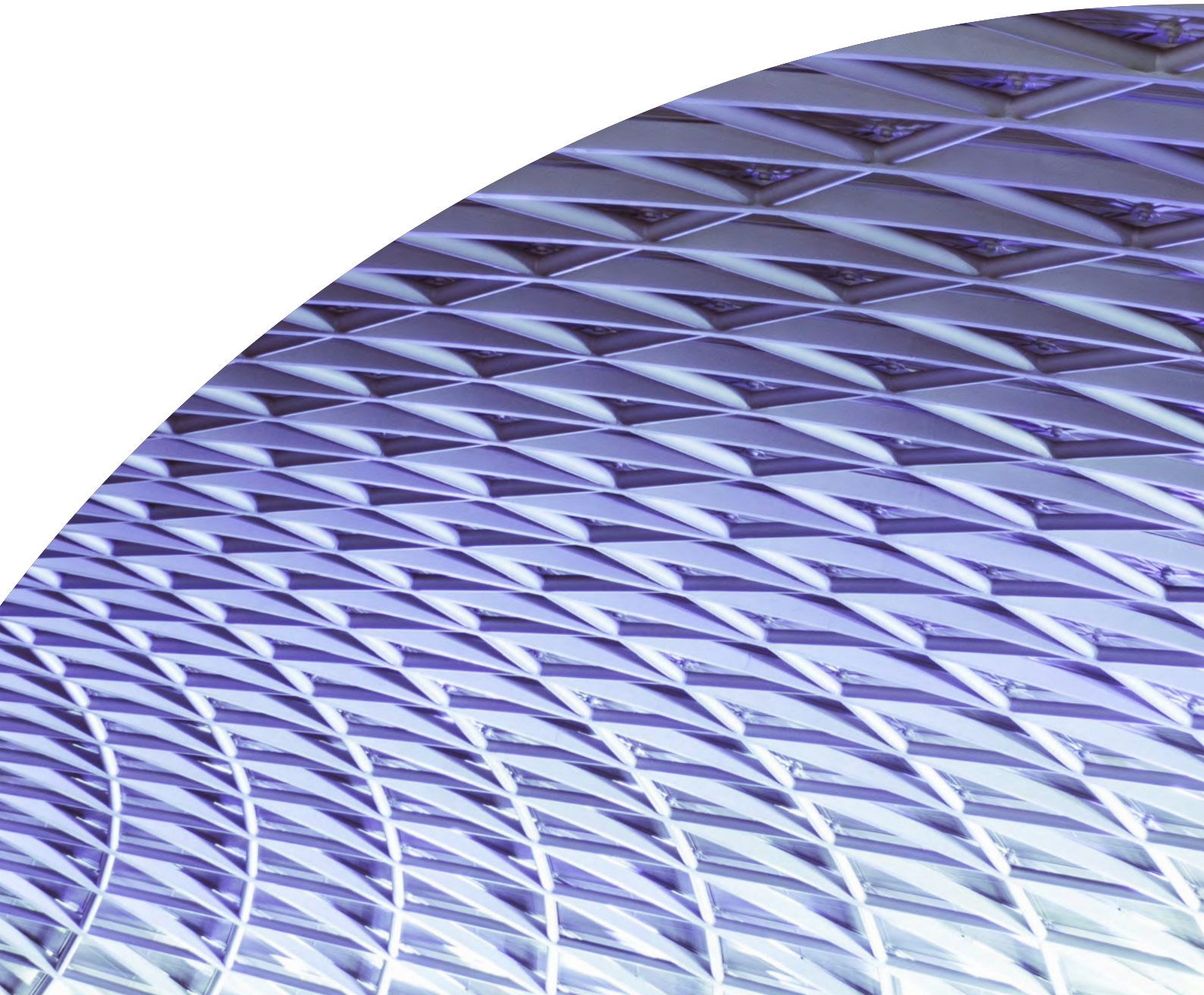
Cyber Security

Sanktionen

Vorbereitung auf die EU-DSGVO

EU-Datenschutz-Grund-verordnung (EU-DSGVO): Zeit zum Handeln

Die wichtigsten Änderungen für Unternehmen



Inhalt

Vorwort

Einführung in die EU-DSGVO

Technischer Fortschritt, wachsende Globalisierung und internationale Verflechtungen sind nur einige Gründe, weshalb es notwendig ist, das Datenschutzrecht in Europa zu harmonisieren. Inwieweit das der EU-Kommission gelungen ist, bleibt zunächst abzuwarten. Die Umsetzung der EU-DSGVO in nationales Recht entfaltet aufgrund von Artikel 288 Absatz 2 AEUV eine unmittelbare und verbindliche Wirkung für jeden Mitgliedsstaat. Nichtsdestotrotz bestehen Regelungsräume in Form von Öffnungsklauseln für beispielsweise Betriebsvereinbarungen, nationale Sondervorschriften und den Beschäftigtendatenschutz.

Mit Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung am 25. Mai 2018 werden zahlreiche nationale Datenschutzregelungen abgelöst und durch ein europäisches Regelwerk zum Schutz personenbezogener Daten ersetzt. Da das Zeitfenster bis zum Stichtag immer kleiner wird, sind Unternehmen angesichts der Komplexität des Themas gut beraten, unbedingt zu prüfen, ob sie den neuen Datenschutzherausforderungen gewachsen sind. Auf der Grundlage von unternehmensspezifischen Risiken muss zunächst ein Aktionsplan entwickelt werden, der das Ziel verfolgt, risikobewertete Lücken zu schließen. Darauf aufbauend ist es notwendig, dass die Datenschutzorganisation über ausreichend Ressourcen und Know-how verfügt. Für eine erfolgreiche Implementierung eines Datenschutzmanagementsystems ist der Rückhalt der Unternehmensführung unerlässlich.

Insbesondere sollte das unternehmerische Risiko im Hinblick auf eine zivilrechtliche Haftung von materiellen und immateriellen Schäden bei der weiteren Umsetzung von Prozessen berücksichtigt werden. Ziel sollte es sein, die Datenschutzorganisation so zu transformieren, dass sie von einem rein operativen Werkzeug zu einem Akteur wird, der die Initiative ergreift. **Sprechen Sie uns an! Gerne entwickeln wir auf Ihr Unternehmen zugeschnittene Lösungen, die Sie überzeugen werden.**

Wir laden Sie herzlich ein, sich auf den folgenden Seiten ein Bild von den Anforderungen der EU-DSGVO und unseren Kompetenzen zu machen.

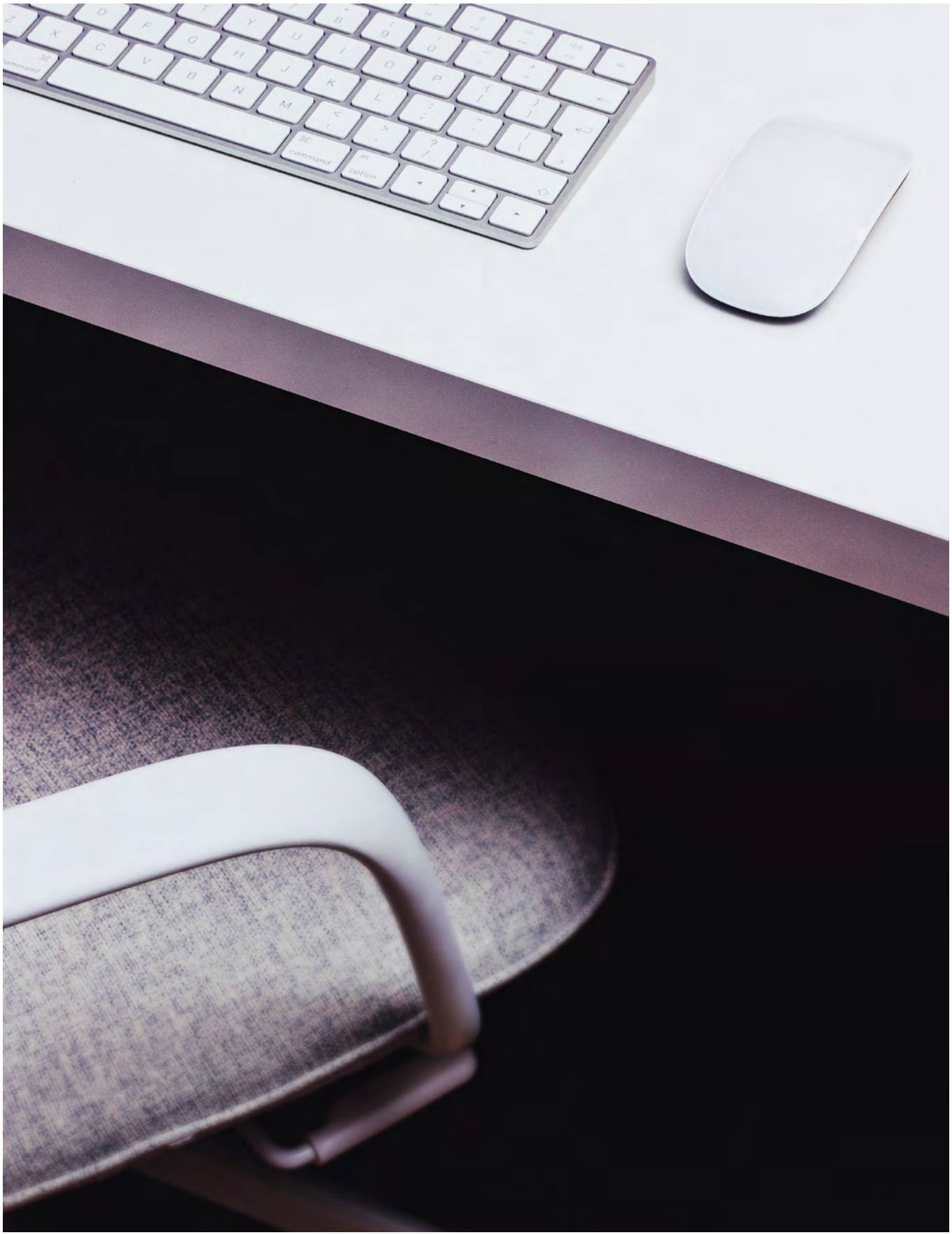
Was müssen Unternehmen beachten?

Prüfen Sie zeitnah, welche Anforderungen der EU-DSGVO bereits heute erfüllt sind und wo noch Handlungsbedarf besteht.

Bitte geben Sie an, was auf Sie zutrifft.	Ja	Nein
Wissen Sie, **wo und in welchen Systemen** in Ihrem Unternehmen personenbezogene Daten gespeichert werden?		
Muss eine **Zustimmung** zur Datenverarbeitung **aktiv** erfolgen? Und wird diese Zustimmung klar und deutlich getrennt von anderen Vereinbarungen dargestellt?		
Ist für jede Verarbeitung personenbezogener Daten schriftlich festgelegt, zu welchem **Zweck** diese erfolgen soll, und wird geprüft, ob die Daten zu einem anderen Zweck weiterverwendet werden dürfen?		
Haben Sie für Ihre Datenverarbeitung eine **Datenschutz-Folgenabschätzung** vorgenommen und dokumentiert?		
Werden **regelmäßige Audits** durchgeführt und Personalrichtlinien sowie Schulungsunterlagen regelmäßig überprüft und gegebenenfalls aktualisiert?		
Sind Ihre Mitarbeiter und Systeme in der Lage, Anfragen zur **Datenlöschung** korrekt zu verarbeiten und umzusetzen?		
Gibt es ein **Datenschutzmanagementsystem**, welches die wirksame Umsetzung der datenschutzrechtlichen Grundsätze dokumentiert und nachvollziehbar die Entscheidungen über die Weiterverarbeitung der Daten und die beeinflussenden Faktoren darstellt?		
Gibt es klare Vorgaben zur Dokumentation und Kommunikation von **Verstößen**?		
Können die erhobenen Daten leicht in **maschinenlesbare Formate** exportiert werden?		
Werden betroffene Personen darüber informiert, dass sie ihre Einwilligung zur Datenvereinbarung **widerrufen** können?		

Haben Sie eine Frage mit „Nein“ beantwortet?

Dann sollten Sie Rat von einem Experten einholen. Kontaktieren Sie uns!



Wichtige Änderungen der EU-DSGVO

Auch wenn der Handlungsbedarf zunächst erdrückend erscheint, bestehen viele Parallelen zwischen der EU-DSGVO und dem Bundesdatenschutzgesetz (BDSG). Neben einigen grundlegenden Änderungen, wie beispielsweise der Einführung eines vollständigen Datenschutzmanagementsystems und eines verschärften Bußgeldrahmens, sind viele Normierungen – in modifizierter Weise – erhalten geblieben.

Verschärfung Bußgeldrahmen

Lag die Bußgeldhöchstgrenze bislang bei 300.000 Euro, erhöht sie sich mit der EU-DSGVO auf 4 % des Konzernumsatzes oder 20 Millionen Euro.

Hinweis: Die individuelle Risikosituation des Unternehmens mit Blick auf Sanktionen aus der EU-DSGVO sollte geprüft werden. Datenschutz erhält im Rahmen der Compliance-Risikoanalyse einen neuen Stellenwert.

Rechenschaftspflichten

Der Verantwortliche hat die Einhaltung der gesetzlichen Pflichten aus der EU-DSGVO nachzuweisen. Hierfür ist ein Datenschutzmanagementsystem unabdingbar.

Hinweis: Datenschutz wird nicht „vom Datenschutzbeauftragten gemacht“, sondern muss in den Unternehmensprozess integriert und beachtet werden.

Verzeichnis von Verarbeitungstätigkeiten

Als zentrales Dokumentationsinstrument zur Datenschutz-Compliance wird das bislang wenig beachtete Verfahrensverzeichnis größere Bedeutung gewinnen. Das Nichtvorhalten ist gemäß BDSG nicht bußgeldbewehrt. Zukünftig drohen hingegen Bußgelder von bis zu 10 Millionen Euro oder 2 % des gesamten weltweiten Vorjahresumsatzes.

Hinweis: Für den Verantwortlichen ergibt sich eine faktische Beweislastumkehr im Hinblick auf den Nachweis. Im Zivilverfahren wird eine Haftungsreduktion nur mit einer gewissenhaften Dokumentation möglich sein.

Datenschutz-Folgenabschätzung

Die im BDSG verankerte Vorabkontrolle wird durch die vielfach umfangreiche Kontrolle der Folgenabschätzung erweitert. Im Rahmen der Risikoanalyse müssen mögliche Folgen für Betroffene abgeschätzt werden.

Hinweis: Die Folgenabschätzung muss mit dem Verzeichnis der Verarbeitungstätigkeiten verknüpft und stets auf dem aktuellen Stand gehalten werden.

Privacy by Design und Privacy by Default

Bei Festlegung der Mittel der Verarbeitung, aber auch bei der Verarbeitung selbst sind technische und organisatorische Maßnahmen zu treffen, um das Ziel der Datenminimierung wirksam umzusetzen. Der Verantwortliche hat geeignete Voreinstellungen vorzunehmen, die sicherstellen, dass ausschließlich personenbezogene Daten verarbeitet werden, die für den Vorgang erforderlich sind.

Betroffenenrechte

Die Rechte der Betroffenen werden durch die EU-DSGVO weiter gestärkt. So sind folgende Neuerungen zu beachten: Anträge müssen innerhalb eines Monats bearbeitet werden; erhobene Daten müssen auf Antrag in einem lesbaren Format an den Betroffenen übermittelt werden; personenbezogene Daten sind unverzüglich zu löschen.

Hinweis: Es müssen Prozesse eingerichtet werden, die die Wahrung der Betroffenenrechte ermöglichen. Die fristgerechte Umsetzung muss zwingend beachtet werden.

Meldepflicht bei Verstößen

Jeder Datenschutzverstoß ist nunmehr der zuständigen Behörde zu melden. Verstöße müssen binnen 72 Stunden nach Bekanntwerden gemeldet werden. Bei schwereren Verstößen muss neben der Aufsichtsbehörde auch der Betroffene informiert werden.

Einführung des Marktortprinzips

Im Rahmen der EU-DSGVO richtet sich die Anwendung nach dem Aufenthaltsort des Betroffenen und nicht nach dem Ort des Verarbeiters.

Einwilligungen

Mit der Nachweispflicht muss sichergestellt werden, dass der Betroffene vor der Datenverarbeitung über den Zweck ausreichend informiert wurde. Für Personen unter sechzehn Jahren muss eine Einwilligung vorliegen. Diese bedarf zu ihrer Wirksamkeit der Zustimmung des Sorgeberechtigten.

Unsere Lösung – ein ganzheitliches Konzept

Warth & Klein Grant Thornton unterstützt Sie mit einem eingespielten Expertenteam rund um das Thema Datenschutz.

Unser Ansatz umfasst drei Phasen: Bestandsaufnahme, Datenschutzkonzept und Umsetzung.

Phase 1: Bestandsaufnahme

In Abstimmung mit Ihnen führen wir eine Bestandsaufnahme des Ist-Zustandes sowie eine Analyse einzelner bereits identifizierter datenschutzrelevanter Risikobereiche und Prozesse durch. Dabei werden vorhandene Prozesse und implementierte Maßnahmen auf mögliche Risiken und Schwachstellen beurteilt. Nach der Bestandsaufnahme zeigen wir vorhandene Lücken auf und erörtern gemeinsam mit Ihnen, inwieweit die Bestimmungen des Datenschutzes durch bestehende Maßnahmen erfüllt werden. Dabei gehen wir auf ausgewählte kritische Punkte ein, die sich aus den gesetzlichen Bestimmungen ergeben.

Phase 2: Datenschutzkonzept

Die Bestandsaufnahme ermöglicht Ihnen, eine zielgerichtete Optimierung – besonders der datenschutzrechtlich kritischen Bereiche – vorzunehmen. Wir unterstützen Sie bei der Erstellung Ihres Datenschutzkonzeptes. Insbesondere erarbeiten wir Handlungsempfehlungen für gegebenenfalls einzuleitende Maßnahmen und unterstützen Sie bei deren Umsetzung.

Phase 3: Umsetzung

Unsere Leistung umfasst die Umsetzung eines Datenschutzkonzeptes in Einzelbereichen (zum Beispiel durch die Erstellung entsprechender Richtlinien und Regelwerke sowie diesbezügliche Schulungen) und die Integration der Datenschutzanforderungen im Unternehmen.

Kontaktieren Sie uns!

Nutzen Sie unser Know-how und unsere Erfahrung – wir freuen uns auf Ihre Fragen.

Warth & Klein Grant Thornton zählt zu den führenden deutschen Wirtschaftsprüfungsgesellschaften. Rund 900 Mitarbeiter betreuten an 10 Standorten einen repräsentativen Querschnitt der deutschen Wirtschaft mit Unternehmen und Institutionen aus nahezu allen Branchen sowie private Vermögensinhaber. In Deutschland verfügen wir im Bereich Governance, Risk & Compliance über ein Team von rund 30 Experten, das Ihnen profundes Know-how und umfassende Unterstützung rund um das Thema Datenschutz bietet.

Auch bei Fragen mit internationalem Bezug müssen Sie nicht auf unsere hohen Qualitätsstandards verzichten. Bei grenzüberschreitenden Sachverhalten arbeiten wir mit dem leistungsstarken Netzwerk Grant Thornton International zusammen. Über 47.000 Mitarbeiter in über 130 Ländern garantieren Ihnen weltweit hervorragenden Service auf einheitlich hohem Niveau – für jede Ihrer Herausforderungen und mit dem richtigen Experten vor Ort.

Ihre Ansprechpartner

WP/StB Dr. Frank Hülsberg
Senior Partner
T +49 211 9524 8527
E frank.huelsberg@wkgt.com

RA Christian Knake
Partner
T +49 211 9524 8572
E christian.knake@wkgt.com

Für mehr Informationen besuchen Sie www.wkgt.com oder schreiben Sie eine E-Mail an datenschutz@wkgt.com.

Impressum
Alle Angaben erfolgen nach bestem Wissen, jedoch ohne Gewähr, und können eine umfassende Beratung im Einzelfall nicht ersetzen.

Redaktionsstand: 01/2018

Herausgeber
Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft
Johannstraße 39
40476 Düsseldorf

T +49 211 9524 0
F +49 211 9524 200

Gestaltung
Seele und UNIMAK GmbH

Warth & Klein Grant Thornton

An instinct for growth™

wkgt.com