www.pwc.de

Löschen personenbezogener Daten nach EU-DSGVO

Erstellung allgemeiner Löschkonzepte als Best Practice.

pwc

Rechtlicher Hintergrund

Der technologische Wandel und die damit verbundene verbesserte Rechen- und Festplattenleistung ermöglichen es, Daten für eine unbegrenzte Dauer zu speichern. Davon profitieren Unternehmen sehr, denn es ermöglicht beispielsweise die Auswertung gesammelter Kundendaten im Rahmen von Marketingmaßnahmen auch noch Jahre später. Das unbegrenzte Sammeln personenbezogener Daten (pbD) jedoch steht im Spannungsfeld mit der **Löschpflicht von pbD**. Wer Daten sammelt, muss diese auch rechtskonform, das heißt in der richtigen Art und Weise und zum richtigen Zeitpunkt, löschen.

Die gesetzlichen Anforderungen an das Löschen bestehen bereits seit der Einführung der EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 und wurden von der europäischen **Datenschutz-Grundverordnung** (DSGVO) vom 25. Mai 2018 lediglich erweitert. Durch die mit der Einführung der DGSVO verbundene hohe Bußgeldandrohung hat sich die Bedeutung der Einhaltung dieser gesetzlichen Anforderungen allerdings drastisch erhöht.

Was in der Theorie einfach klingt, stellt in der Praxis eine Herausforderung dar, denn Unternehmen verarbeiten eine Vielzahl an verschiedenen Daten in unterschiedlichsten IT-Systemen und müssen somit unterschiedliche Lösch- und Speicherpflichten beachten. Hieraus ergibt sich die Notwendigkeit der Erstellung eines **allgemeinen Löschkonzepts**, das die Art und Weise, wie pbD im Unternehmen gelöscht werden, regelt. So wird die Einhaltung der Rechtsvorgaben der DSGVO sichergestellt.

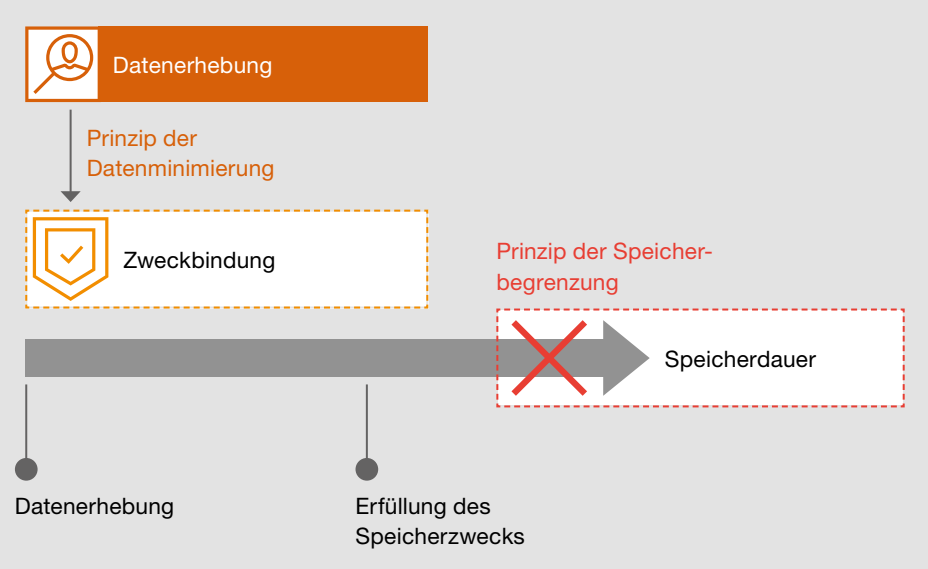
Hierbei ist besonders darauf zu achten, dass die einzelnen IT-Systeme im Hinblick auf das Löschen nicht getrennt voneinander betrachtet werden. Vielmehr ist eine **übergeordnete Herangehensweise**, die die **Rahmenbedingungen** für die einheitliche Umsetzung in einzelnen IT-Systemen schafft, essenziell.

Die Erstellung eines solchen Löschkonzepts kann für Unternehmen als Chance betrachtet werden, die eigenen Geschäftsprozesse kritisch zu durchleuchten, gegebenenfalls **effizienter** zu gestalten und ein **positives Datenschutzimage** zu kreieren. Darüber hinaus kann durch eine Reduzierung von Daten eine bessere Performance und Stabilität von IT-Systemen erzielt werden.

1 Grundsätze der Datenminimierung und Speicherbegrenzung

In Artikel 5 sieht die DSGVO mehrere sogenannte Grundsätze für die Zulässigkeit der Verarbeitung von pbD vor. Drei dieser grundlegenden Prinzipien sind die **Zweckbindung**, die **Datenminimierung** und die **Speicherbegrenzung**. Welche Beziehung diese drei Prinzipien zueinander haben, ist in Abbildung 1 ersichtlich.

Abb. 1 Prinzipien der Datenverarbeitung



Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) meint, dass pbD nur für einen bestimmten Zweck verarbeitet werden dürfen. Zudem dürfen ausschließlich diejenigen Daten erhoben und verarbeitet (und somit auch gespeichert) werden, die für den Zweck der Verarbeitung notwendig sind (**Datenminimierung** Art. 5 Abs. 1 lit. c DSGVO).

Der Grundsatz der **Speicherbegrenzung** unterstützt die Datensparsamkeit in Bezug auf die Dauer der Speicherung. Demnach dürfen pbD nur so lange gespeichert werden, wie dies zur Erfüllung des Speicherzwecks notwendig ist (Art. 5 Abs. 1 lit. e DSGVO). Nach Wegfallen dieses Zwecks sind pbD dauerhaft unkenntlich zu machen.

Aus diesen drei Prinzipien resultiert die Notwendigkeit, eine Löschung von pbD umzusetzen. Dies wird ebenso durch das **Recht des Betroffenen auf Löschung** sichergestellt, das in Artikel 17 DSGVO verankert ist. Im Rahmen der Löschung wird zwischen der regelmäßigen und anlassbezogenen (außerordentlichen) Löschung unterschieden. Bei der regelmäßigen Löschung wird der Löschprozess durch das Unternehmen auf eigene Initiative im Rahmen seiner Geschäftsprozesse angestoßen (Grundsatz der Speicherbegrenzung).

Bei der anlassbezogenen Löschung hingegen wird der Löschprozess durch ein Ereignis, wie beispielsweise die Geltendmachung des Rechts auf Löschung, ausgelöst, das in der Regel von einem Betroffenen an das Unternehmen herangetragen wird.

2 Dokumentation (Rechenschaftspflicht)

Ein weiterer für Unternehmen relevanter Grundsatz ist die **Rechenschaftspflicht** (Art. 5 Abs. 2 DSGVO). Um dieser Rechenschaftspflicht nachkommen zu können, ist eine umfangreiche Dokumentation von Löschvorgaben, auch über die Grenzen vereinzelter IT-Systeme hinaus, unerlässlich. Hierfür ist eine übergreifende Dokumentation von besonderer Bedeutung, da nur so sichergestellt werden kann, dass eine einheitliche Methodik für alle Systeme angewendet wird. Zudem ergibt sich durch die unterschiedlichen Lösch- und Aufbewahrungsfristen eine Komplexität, die nur durch ein übergreifendes allgemeines Löschkonzept aufgearbeitet werden kann.

Neben der Festlegung der Regeln zur Löschung von pbD stellt die Dokumentation eine wichtige Grundlage für die Beantwortung von Anfragen durch Aufsichtsbehörden dar.

Aufbau eines allgemeinen Löschkonzepts

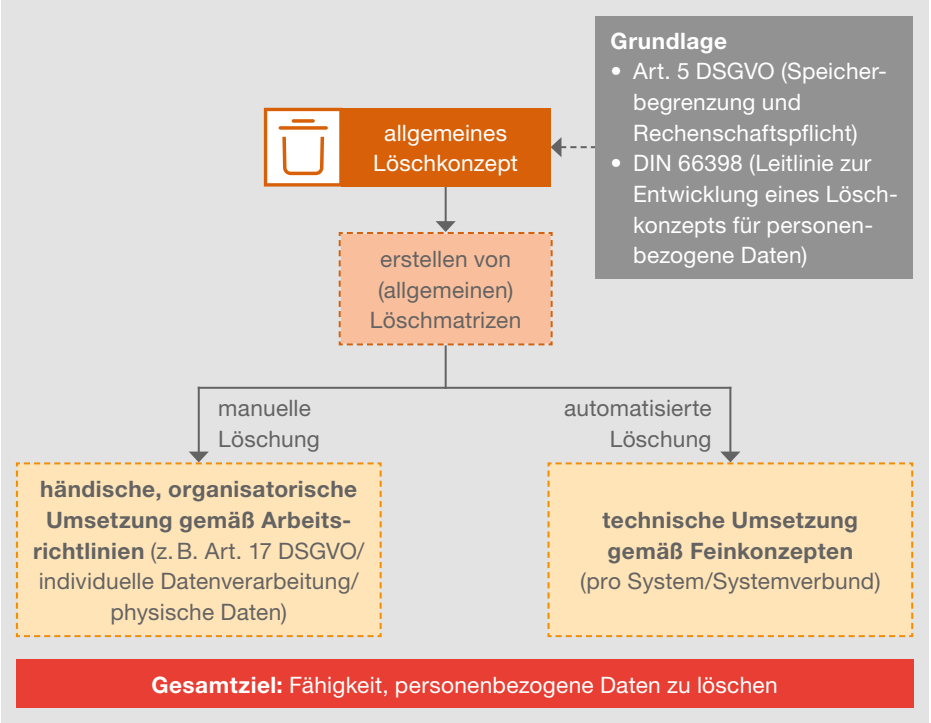
Für die Erstellung eines allgemeinen Löschkonzepts empfiehlt sich eine Orientierung an der **DIN-Norm 66398**. Diese beschreibt die Vorgehensweise zur Erstellung eines Löschkonzepts und gibt speziell Hinweise zu Inhalt, Aufbau und Verantwortlichkeiten in Bezug auf das Löschen. Die Erfahrung zeigt, dass diese Vorgehensweise besonders geeignet ist, um ein ganzheitliches Löschkonzept in einer Organisation für eine komplexe IT-Landschaft zu etablieren.

Um die Vorgaben der DIN-Norm optimal umzusetzen, empfiehlt sich eine Aufteilung des allgemeinen Löschkonzepts in einen theoretischen Teil mit Begriffserklärungen und Beschreibung der Methodik sowie einen unternehmensspezifischen Teil, in dem die konkrete Umsetzung im Unternehmen beschrieben wird. Diese Ausführungen werden gefolgt von einer praktischen Anleitung zur Erstellung von konkreten Löschmatrizen. Ein solches allgemeines Löschkonzept stellt das Grundgerüst für das Löschen von pbD im Unternehmen dar.

Neben der Erstellung eines allgemeinen Löschkonzepts erfordert ein datenschutzkonformer Umgang mit dem Löschen auch die organisatorische Umsetzung von manuellen Löschprozessen sowie die technische Implementierung von Löschroutinen.

Das Zusammenspiel der unterschiedlichen Aspekte des Löschens ist in Abbildung 2 dargestellt.

Abb. 2 Grundlagen des Löschkonzepts



1 Theoretischer Teil des Löschkonzepts

Der theoretische Teil des Löschkonzepts sollte die Grundlagen beschreiben, die fundamental für das Verständnis des Löschens sowie des weiteren Vorgehens sind.

Zentraler Bestandteil dieses Abschnitts sollte die Aufarbeitung der theoretischen Grundlagen sowie eine „Übersetzung“ der gebräuchlichen Begriffe in die jeweilige Unternehmenssprache sein.

Zusätzlich sollte eine **Methodik** nach DIN 66398 entwickelt werden, die ein einheitliches Verständnis für ein beispielhaftes Vorgehen ermöglicht. Ziel ist die datenschutzkonforme Löschung durch einen einheitlichen Umgang mit pbD sicherzustellen. Um dies zu erreichen, werden nach der DIN 66398 die Daten in einer strukturierten Darstellung zusammengefasst. Zu Beginn werden Daten, die für denselben Zweck verarbeitet werden, zu sogenannten **Datenarten** zusammengefasst. Beispielsweise können die Daten „Name“, „Vorname“ und „Geburtsdatum“ unter anderem der Datenart „Bewerberdaten“ angehören. Im Anschluss wird festgelegt, wann diese Daten gelöscht werden müssen (Löschfrist). Um den Löschvorgang zu strukturieren, werden Datenarten mit der gleichen **Löschfrist** in Löschklassen zusammengefasst. Damit eine Fristberechnung möglich ist, wird am Ende festgelegt, wann die Frist zu laufen beginnt. Hieraus leitet sich die eigentliche **Löschregel** für eine Löschklasse ab.

2 Unternehmensspezifischer Teil des Löschkonzepts

Auf die theoretischen Grundlagen sollte ein unternehmensspezifischer Teil folgen. Hier sollte konkretisiert werden, wie die zuvor beschriebene Methodik im Unternehmen angewendet wird.

Konkret können in Unternehmen neben der automatisierten Verarbeitung von pbD im Rahmen von spezifischen IT-Systemen folgende Bereiche betroffen sein: nicht systemspezifische IT-Prozesse sowie manuelle Prozesse.

Zum einen sollte der unternehmensspezifische Teil Angaben über die **IT-Systeme**, die für die Verarbeitung von pbD von zentraler Bedeutung sind, enthalten. Eine Implementierung automatisierter Löschvorgänge für pbD in diesen IT-Systemen kann im Löschkonzept dokumentiert werden.

Zum anderen sollten Vorgehensweisen zur **nicht systemspezifischen Umsetzung** im Löschkonzept festgelegt werden. Eine nicht systemspezifische Umsetzung liegt unter anderem im Fall von Sicherungskopien, Archiv- und Testsystemen vor. Beispielsweise werden Sicherungskopien genutzt, um Systeme und Datenbestände nach Störungen wiederherzustellen. Sie dürfen daher nicht verändert werden und auch eine Löschung innerhalb einer Backup-Generation widerspricht dem Zweck einer Sicherung. In diesem Fall ist zur Zweckerreichung jedoch nur eine geringe Vorhaltezeit notwendig. Mit kurzen Löschfristen für die Backup-Generationen kann den Löschvorgaben entsprochen werden.

Zudem wird beschrieben, wie in Fällen, in denen eine unmittelbare Löschung beispielsweise aufgrund einer gesetzlichen Aufbewahrungspflicht oder die Möglichkeit zur Durchsetzung von Ansprüchen nicht möglich ist, verfahren wird. Hier ist eine **Einschränkung der Verarbeitung** erforderlich. Darunter wird aus prozessualer Sicht die Beschränkung der Zugriffsrechte auf pbD verstanden. Dadurch wird der Zugriff auf diese gesperrten pbD nur noch insoweit ermöglicht, wie dies zur Erfüllung des jeweiligen Zwecks erforderlich ist.

3 Anleitung zur Erstellung von Löschmatrizen

Des Weiteren sollte das Löschkonzept eine Anleitung zur Erstellung von **Löschmatrizen** enthalten, die auf den Informationen des allgemeinen und unternehmensspezifischen Teils aufbaut.

Eine Löschmatrix ist eine kompakte Darstellungsweise der gesetzlichen Anforderungen, denen pbD in bestimmten Verarbeitungstätigkeiten oder IT-Systemen unterworfen sind. Diese Löschmatrix dient der Identifikation von Löschregeln, die technisch oder durch manuelle Prozesse (z. B. durch die Mitarbeiter) umgesetzt werden sollten.

Im Rahmen der Erstellung eines allgemeinen Löschkonzepts empfiehlt es sich, eine allgemeine Löschmatrix zu entwickeln, die anhand beispielhafter Datenarten aufzeigt, wie die Löschanforderungen innerhalb des Unternehmens umgesetzt werden sollen. Diese Anwendungshilfe soll es dem jeweiligen Fachbereich erleichtern, eine spezifische, seinen Anforderungen entsprechende Löschmatrix zu erstellen.

4 Manuelle Löschung

Neben der Umsetzung in den IT-Systemen und der nicht system-spezifischen Umsetzung existiert ein weiteres Umsetzungsfeld im Bereich der **manuellen Löschung** (siehe Abbildung 3).

Da in bestimmten Sondersituationen keine zentralen Löschmechanismen implementiert werden können, sollten manuell durchzuführende Lösch-prozesse definiert werden.

Umgang mit individueller Daten-verarbeitung

Unter **individueller Datenverarbeitung** wird die Verarbeitung pbD außerhalb der automatisierten Regelprozesse unter dem Einsatz von Endanwender-Software verstanden (z. B. Microsoft-Office-Lösungen). In diesem Fall hat der Anwender eine Auswahlmöglichkeit hinsichtlich der Ablagemöglichkeiten der Daten und somit existiert kein fest vorgegebener Speicherort. Hier können Arbeitsanweisungen erstellt werden, um den Mitarbeitern anhand organisatorischer Regelungen den ordnungsgemäßen Umgang mit datenschutzrechtlichen Anforderungen zu erleichtern. Konkret können diese unter anderem Regeln zur Weitergabe individuell verarbeiteter Daten, Regeln zur Ablage von Datenauszügen und Schutzmaßnahmen vor unbefugtem Zugriff beinhalten.

Umgang mit physischer Datenverarbeitung

Physische Datenverarbeitung bezeichnet die Handhabung von papierhaften Unterlagen und den Einsatz von digitalen Speichermedien. Auch in diesem Fall können Arbeits-anweisungen erstellt werden, die Vorgaben zur Aufbewahrung und Entsorgung papierhafter Unterlagen oder externer Speichermedien wie USB-Sticks machen. Hierbei empfiehlt es sich, die besonderen Vorgaben der DIN 66399, die je nach Schutzbedarf der Daten ein individuelles und angemessenes Löschverfahren für Datenträger festlegen, zu berücksichtigen.

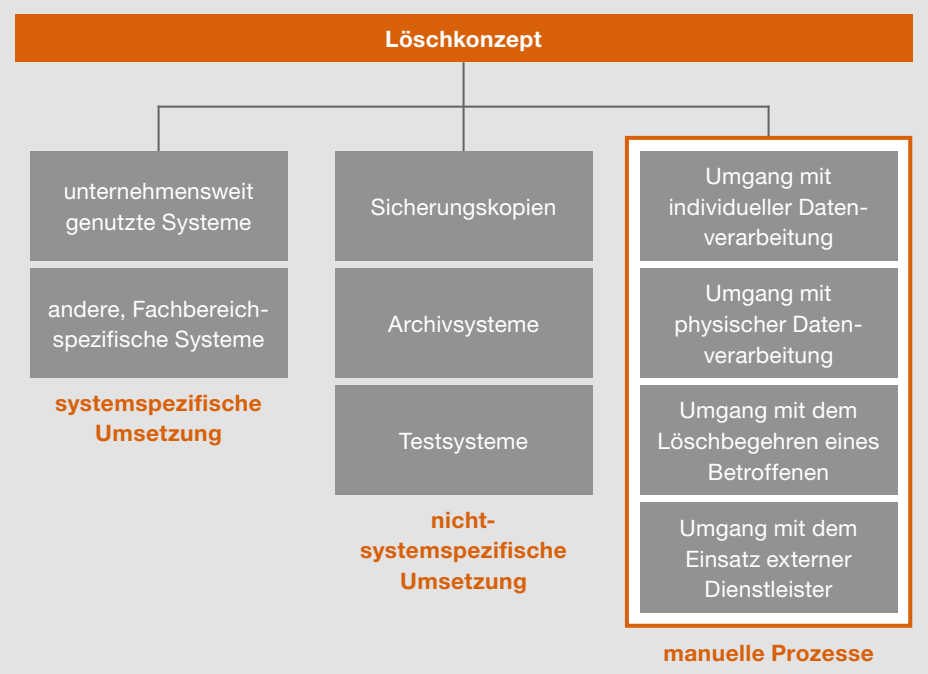
Umgang mit dem Löschbegehren eines Betroffenen

Der Betroffene hat gemäß Artikel 17 DSGVO in bestimmten Fällen das Recht, vom Unternehmen die Löschung seiner pbD zu verlangen. Hier sollte ein Prozess zur Prüfung und Bearbeitung der Betroffenenanfrage definiert und dokumentiert werden.

Umgang mit dem Einsatz externer Dienstleister

Werden im Rahmen der Auftrags-verarbeitung externe Dienstleister eingesetzt, muss berücksichtigt werden, dass die Löschpflicht auch die pbD umfasst, die bei den Dienstleistern verarbeitet werden. Hierfür müssen die Verantwortlichkeiten und Fristen zur Löschung von pbD im Auftrags-verarbeitungsvertrag geregelt und regelmäßig durch den Auftraggeber, beispielsweise durch entsprechende Auditierungen, kontrolliert werden.

Abb. 3 Umsetzungsbereiche des allgemeinen Löschkonzeptes



Vorgehen zur Erstellung eines allgemeinen Löschkonzepts

1 Zuweisung von Verantwortlichkeiten

Die Erstellung eines allgemeinen Löschkonzepts erfordert die Zusammenarbeit zwischen dem Fachbereich, der für das Datenverarbeitungsverfahren verantwortlich ist, der zuständigen IT und dem Datenschutzbeauftragten sowie der Rechtsabteilung, um die erforderlichen umsetzungsrelevanten Anforderungen fachlich, technisch und rechtlich festzulegen.

Es empfiehlt sich daher, den Prozess der Umsetzung der Löschvorgaben als umfassendes und fachbereichsübergreifendes Projekt durchzuführen. Im Rahmen der Projektplanung sollte eine entsprechende Ressourcenplanung vorab durchgeführt werden. Nur so können neben den datenschutzrechtlichen Vorgaben auch erfolgreich entsprechend unternehmensinterne Vorgaben umgesetzt werden.

2 Projektverlauf

Der Projektverlauf der Erstellung eines allgemeinen Löschkonzepts sollte sich am Aufbau des allgemeinen Löschkonzepts orientieren. Der Projektverlauf besteht aus der Phase der Konzeption und der Phase einer Analyse und Bewertung der IT-Systemlandschaft. In der Konzeptionsphase erfolgt die Festlegung des Inhalts für den theoretischen Teil des Löschkonzepts. Hier werden die im Unternehmen gebräuchlichen Begriffe definiert und die Vorgehensweise allgemein beschrieben. Zu Beginn der zweiten Phase werden die vorhandenen IT-Systeme analysiert und Datenarten sowie Aufbewahrungsfristen identifiziert. Hierzu empfiehlt sich die Einbeziehung der Fachbereiche sowie der Rechtsabteilung.

Auf Basis der hieraus gewonnenen Erkenntnisse werden konkrete Umsetzungsvorgaben entwickelt. Die Erstellung beispielhafter Löschmatrizen erfolgt auf Grundlage der zuvor festgelegten Rahmenbedingungen. Hier sollte neben dem Datenschutzbeauftragten auch die IT-Abteilung involviert werden.

Im Anschluss an die Erstellung des allgemeinen Löschkonzepts erfolgt die Erstellung systemspezifischer Löschkonzepte inklusive der technischen Umsetzung in den IT-Systemen durch einen IT-Dienstleister.

Ein exemplarischer Projektverlauf ist in Abbildung 4 dargestellt:

Abb. 4 Projektablauf zur Erstellung des allgemeinen Löschkonzepts

Unser Beitrag

Die Berücksichtigung aller oben beschriebenen Aspekte macht die Umsetzung der Rechtsvorgaben zum Thema Löschen zu einem sehr komplexen Handlungsfeld, das Unternehmen sowohl vor eine rechtliche als auch vor eine organisatorische Herausforderung stellt.

Um dieser Herausforderung bei der Erstellung eines Löschkonzepts erfolgreich zu begegnen, bieten wir unsere Unterstützung in folgenden Bereichen an und entwickeln individuelle und bedarfsgerechte Lösungen für Ihr Unternehmen:

- **Prüfung des allgemeinen Löschkonzepts** mit Empfehlungen und gegebenenfalls Überarbeitung
- Erstellung einer **individuellen Vorlage** für ein allgemeines Löschkonzept
- **Unterstützung bei der Erarbeitung eines vollständigen allgemeinen Löschkonzepts** für Ihr Unternehmen
- **Unterstützung bei Fragestellungen** in Bezug auf das Thema Löschen
- **Auditierung Ihrer externen Dienstleister** in Bezug auf das Thema Löschen

Legen Sie noch heute einen wesentlichen Grundstein für die Datenschutzkonformität Ihres Unternehmens und profitieren Sie von unserer langjährigen Datenschutzexpertise aus einer Vielzahl unterschiedlicher Branchen!

Bei weiteren Fragen stehen Ihnen Christian Bartmann und sein Team gern jederzeit zur Verfügung.

Ihr Ansprechpartner

Christian Bartmann
Partner Risk Assurance Solutions,
PwC Germany
Tel.: +49 69 9585-2848
christian.bartmann@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 158 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. Mehr als 11.000 engagierte Menschen an 21 Standorten. 2,2 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.