ADVANT Beiten

Liebe Leserinnen, liebe Leser,

in der aktuellen Ausgabe unseres „Blickpunktes Öffentlicher Sektor" informieren wir Sie wieder über die neusten Themen und Entwicklungen für die Praxis der öffentlichen Hand. Dabei stellen wir Ihnen unsere Experten im Datenschutz vor, die in dieser Ausgabe im Fokus stehen.

Unsere Kollegen aus dem Datenschutz-Team beraten und unterstützen deutschlandweit die öffentliche Hand, Verwaltung und Behörden bei IT- und datenschutzrechtlichen Fragen. Ihre Expertise reicht von komplexen IT-Projekten, der Gestaltung von Datenschutzerklärungen, Richtlinien oder Einwilligungen, bis hin zur Sofort-Hilfe bei Datenpannen einschließlich der Kommunikation mit den Aufsichtsbehörden.

Im Jahr 2025 haben sich in Deutschland entscheidende Entwicklungen im Bereich Datenschutz ergeben, insbesondere im öffentlichen Sektor und in der Verwaltung. Die neue Bundesregierung aus CDU/CSU und SPD verfolgt eine Neuausrichtung der Datenschutzpolitik mit dem Ziel, eine datenschutzkonforme, aber zugleich innovationsfreundliche Verwaltung zu schaffen. Die Digitalisierung der Verwaltung und Justiz ist ein Kernanliegen der neuen Bundesregierung, das unter anderem durch den Einsatz von Künstlicher Intelligenz erreicht werden soll (siehe dazu den Blogbeitrag von Fabian Eckstein vom 2. Mai 2025).

Die KI-Verordnung ist bereits in wesentlichen Teilen in Kraft getreten und verpflichtet öffentliche Stellen, die KI-Systeme einsetzen wollen, u.a. zur Schulung ihrer Beschäftigten und zur Prüfung eingesetzter KI-Systeme auf verbotene Praktiken. Vermehrt sind wir zuletzt auch mit der Erstellung von KI-Richtlinien befasst, um für die Beschäftigten einen Verhaltenskodex im Umgang mit KI zu etablieren. Das BSI hat 2025 flankierend einen Kriterienkatalog sowie einen Leitfaden für den Einsatz von KI in der Verwaltung veröffentlicht, die Jason Komninos in diesem „Blickpunkt" näher vorstellt.

Auch die im April 2025 in Kraft getretene Einwilligungsverordnung, bringt Veränderungen: Sie erlaubt es Nutzern von Webseiten und sonstigen Online-Diensten, ihre Datenschutz-Einwilligungen zentral über spezialisierte Anbieter zu verwalten. Ziel ist es, die allgegenwärtigen Cookie-Banner überflüssig zu machen und die Kontrolle über personenbezogene Daten zu stärken – bei gleichzeitiger Vereinfachung für Diensteanbieter.

Nach wie vor höchst aktuell ist die Frage, welche technischen und organisatorischen Maßnahmen ein Verantwortlicher – sei es Unternehmen oder Behörde – ergreifen muss, um den datenschutzrechtlichen Anforderungen zu genügen. Wie sich die Gerichte in Nordrhein-Westfalen zur Frage einer eventuell notwendigen Ende-zu-Ende-Verschlüsselung positioniert haben, erläutert Mirjam Kaiser in diesem „Blickpunkt".

Zuletzt weisen wir auf den ab dem 12. September 2025 anwendbaren Data Act hin, der auch spezifische Regelungen dazu enthält, unter welchen Voraussetzungen staatliche Stellen Zugang zu Daten des Privatsektors verlangen können.

Gerne stehen wir Ihnen für alle Fragen zu den oben genannten Themen, den Beiträgen in diesem Newsletter oder allen sonstigen IT- und datenschutzrechtlichen Fragen zur Verfügung.

Herzliche Grüße

Ihr Team Public Sector von
ADVANT Beiten

Spotlight

In jeder Ausgabe unseres Newsletters stellen wir Ihnen Kolleginnen und Kollegen verschiedener Rechtsgebiete vor. Dieses Mal aus dem Datenschutz:

Susanne Klein, LL.M.
Rechtsanwältin,
Fachanwältin für
Informationstechnologierecht
vCard

Katharina Mayerbacher
Rechtsanwältin,
Fachanwältin für
Informationstechnologierecht
vCard

Mathias Zimmer-Goertz
Rechtsanwalt
vCard

Lennart Kriebel
Rechtsanwalt
vCard

Christian Frederik Döpke, LL.M.
Rechtsanwalt
vCard

Fabian Eckstein, LL.M.
Rechtsanwalt
vCard

Jason Komninos, LL.M.
Rechtsanwalt, Fachanwalt für
Informationstechnologierecht
vCard

Mirjam Kaiser
Rechtsanwältin
vCard

Themen

TOP-THEMA: DATENSCHUTZ

ARBEITSRECHT

ENERGIERECHT

PROZESSFÜHRUNG

Weitere Informationen zu unserer Expertise rund um die Öffentliche Hand finden Sie auf unserer Webseite:

Public Sector

Termine

9. Oktober	**Webinar: Kundenanlagen-Entscheidung des BGH vom 13. Mai 2025** Webinar | 11:00-13:00 Uhr	Einladung
15. Oktober	**Forum ADVANT Berlin 2025** ADVANT Beiten Berlin| ab 17:00 Uhr	Einladung

Weitere Veranstaltungen zu verschiedenen Themen finden Sie auf unserer Webseite:

Veranstaltungen

REDAKTION (verantwortlich)

Hans Georg Neumeier
Dr. Sebastian Kroll

Hinweis: Zur besseren Lesbarkeit verzichten wir auf die Verwendung männlicher und weiblicher Sprachformen. Wir verwenden das generische Maskulinum, womit alle Geschlechter gleichermaßen gemeint sind.

TOP-THEMA

Leitlinien und Vorgaben zum Einsatz von KI in der Verwaltung

Im März 2025 hat das Bundesministerium des Innern und für Heimat (BMI) in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Leitlinien für den Einsatz Künstlicher Intelligenz (KI) in der Bundesverwaltung veröffentlicht. Ergänzend hat das BSI im Juni 2025 einen Kriterienkatalog zum Einsatz von generativer KI in der Bundesverwaltung herausgebracht.

Auch wenn sich beide Papiere zunächst an die Bundesverwaltung richten, ist der Inhalt ohne Weiteres auf die gesamte Verwaltung und die öffentliche Hand übertragbar. Aus diesem Grund fassen wir nachfolgend den Inhalt dieser Papiere für Sie zusammen.

1. Leitlinien für den Einsatz von KI in der Bundesverwaltung

Die Leitlinien bieten erstmals einen umfassenden, wertebasierten Handlungsrahmen für den KI-Einsatz in deutschen Bundesbehörden. Ziel ist es, Chancen der KI-Technologien verantwortungsvoll und sicher zu nutzen, insbesondere vor dem Hintergrund sensibler Daten, staatlicher Verantwortung und öffentlicher Transparenz.

Die Leitlinien beruhen auf fünf übergeordneten Prinzipien, die für alle Behörden verbindlich sind:

- **Chancenorientierter und verantwortungsvoller Einsatz** – KI soll dort eingesetzt werden, wo sie zur Verbesserung staatlicher Leistungen beiträgt.
- **Menschenzentrierung** – Die Technik soll dem Menschen dienen, nicht ihn ersetzen. Entscheidungen bleiben grundsätzlich in menschlicher Verantwortung.
- **Vertrauenswürdigkeit** – KI-Systeme müssen rechtmäßig, ethisch, technisch robust und sozial nachvollziehbar gestaltet sein.
- **Kompetenzförderung** – Mitarbeiterinnen und Mitarbeiter sind durch Schulungen aufzuklären und zu befähigen, KI-Systeme kompetent und kritisch zu nutzen.

- **Nachhaltigkeit** – Technologische, ökologische und soziale Aspekte sind bei der Entwicklung und Beschaffung von KI-Lösungen zu berücksichtigen, ebenso wie die Vermeidung von Anbieterabhängigkeiten (sog. „Lock-in-Effekte").

Inhaltlich gliedern sich die Leitlinien in zwei Bereiche:

a) Leitsätze für Nutzende (A1–A5):

Diese richten sich an Beschäftigte, die mit KI-Systemen arbeiten. Sie fordern u. a. dazu auf, KI ethisch verantwortungsvoll einzusetzen, sensible Daten nur nach Freigabe einzugeben, generierte Inhalte stets fachlich zu prüfen und den KI-Einsatz transparent zu machen. Besonders betont wird der Schutz personenbezogener oder vertraulicher Daten. Die Eingabe solcher Informationen ist nur in speziell freigegebenen, sicheren Umgebungen zulässig.

b) Leitsätze für Behörden (B1–B9):

Hier werden Anforderungen an Leitung, IT-Verantwortliche und Fachabteilungen formuliert. Dazu gehören klare Zuständigkeiten, die Festlegung des Einsatzzwecks, die Auswahl geeigneter und sicherer Systeme, die Berücksichtigung ethischer Aspekte und der Aufbau einer umfassenden Schulungsinfrastruktur. Auch die Nutzung des KI-Marktplatzes der Bundesverwaltung („MaKI") wird zur Transparenzförderung empfohlen.

Zudem enthalten die Leitlinien detaillierte technische und organisatorische Anforderungen, insbesondere zur Informationssicherheit, zur Minimierung der Datenpreisgabe (z. B. durch pseudonymisierte Konten) und zur Kontrolle der eingesetzten KI-Systeme. Ein eigenes Kapitel befasst sich mit dem Einsatz großer Sprachmodelle (LLMs) wie ChatGPT – dieser ist grundsätzlich zulässig, sofern er mit der gebotenen fachlichen und datenschutzrechtlichen Sorgfalt erfolgt.

Die KI-Leitlinien sind damit ein bedeutender Schritt hin zu einem strukturierten, verantwortungsvollen Umgang mit KI in der Verwaltung. Sie sollen nicht nur Handlungssicherheit geben, sondern auch als Grundlage für künftige Regelwerke dienen. Da technologische Entwicklungen fortlaufend stattfinden, verstehen sich die Leitlinien als dynamisches Dokument, das fortgeschrieben werden soll.

2. Kriterienkatalog zum Einsatz von KI in der Bundesverwaltung

Der Kriterienkatalog des BSI zum Einsatz generativer KI in der Bundesverwaltung gibt erstmals einen strukturierten, lebenszyklusorientierten Rahmen für Behörden vor, die externe generative KI-Modelle – etwa große Sprachmodelle wie ChatGPT – in eigene Anwendungen integrieren möchten. Ziel ist es, ein Mindestmaß an Informationssicherheit und Vertrauenswürdigkeit sicherzustellen, dass dem besonderen Schutzbedarf staatlicher Daten und Prozesse gerecht wird. Der Katalog umfasst sämtliche Phasen eines KI-Projekts – von der Planung über die Beschaffung und Integration bis zum Betrieb und zur Beendigung – und enthält sowohl technische als auch organisatorische Anforderungen.

Globale KI-Governance

Bereits vor dem eigentlichen Projektstart sind Behörden verpflichtet, eine zentrale Governance-Struktur für den KI-Einsatz zu schaffen. Dazu gehört insbesondere die Benennung einer oder eines Verantwortlichen, die bzw. der sämtliche KI-Aktivitäten in der Organisation koordiniert. Ebenso ist eine vollständige Übersicht über alle KI-Anwendungen zu führen, inklusive verantwortlicher Stellen, genutzter Modelle und zugelassener Anwendungsbereiche. Schulungen zur Sensibilisierung und Qualifizierung der Beschäftigten im Umgang mit KI-Systemen sind verpflichtend vorzusehen, ebenso wie klare, leicht zugängliche interne Regelungen zur erlaubten Datenverarbeitung.

Planungsphase

In der Planungsphase muss jede Anwendung klar beschrieben und begründet werden. Dabei ist eine Risikoanalyse durchzuführen, die insbesondere typische Risiken generativer KI berücksichtigt – etwa das sog. Halluzinieren falscher Inhalte, die ungewollte Preisgabe sensibler Informationen oder der Missbrauch durch manipulierte Eingaben. Auf Grundlage dieser Bewertung werden konkrete Anforderungen an das zu beschaffende Modell formuliert.

Beschaffungsphase

Die Beschaffungsphase verlangt, dass nur vertrauenswürdige Modelle über nachvollziehbare, vorzugsweise zertifizierte Quellen bezogen werden.

Anbieter müssen vertraglich zusichern, dass eingegebene Daten nicht für Trainingszwecke oder andere Weiterverwendungen genutzt werden.

Anpassungsphase

Bei der Anpassung der KI-Systeme innerhalb der eigenen Anwendung – etwa durch sog. System-Prompts, zusätzliche Werkzeuge oder Anbindungen an Datenbanken – sind besondere Vorsichtsmaßnahmen zu treffen. Wichtig ist, dass keine sensiblen Daten in Prompts vorkommen dürfen und dass Schutzmechanismen gegen Manipulationen wie Prompt Injections berücksichtigt werden.

Integrationsphase

Im Zuge der technischen Integration ist das KI-System in das behördliche Informationssicherheits-Managementsystem (ISMS) einzubinden. Kritische Schnittstellen, Benutzerrechte, Eingabe- und Ausgabekontrollen sowie Logging- und Sandboxing-Maßnahmen sind auf Basis eines Bedrohungsmodells zu entwickeln und umzusetzen. Vor der Inbetriebnahme sind umfassende Tests auf Grundlage der Risikobewertung durchzuführen und zu dokumentieren.

Einsatzphase

Im laufenden Betrieb muss der Einsatz der KI für Nutzende transparent sein. Der Zugriff auf das System ist auf autorisierte Personen zu beschränken und es müssen Maßnahmen zur Missbrauchsvermeidung eingerichtet sein – etwa gegen die automatisierte Generierung falscher Inhalte oder den Zugriff auf vertrauliche Informationen. Weiterhin wird empfohlen, Support- und Hilfsangebote bereitzustellen und Nutzende regelmäßig fortzubilden.

Beendigungsphase

Auch das Ende des Einsatzes ist klar geregelt. Vor der Verwendung für einen anderen Anwendungsfall sind sensible Daten zu löschen, wenn der Einsatzzweck geändert wird. Bei Cloud-basierten Lösungen sind zusätzlich die BSI-Mindeststandards zur Cloud-Nutzung einzuhalten.

Anhang: Typische KI-Risiken

Der Kriterienkatalog wird ergänzt durch einen Anhang, der typische sicherheitsrelevante Risiken generativer KI-Modelle systematisch auflistet

und Hinweise zur Risikobewertung gibt. Dazu zählen u.a. Datenschutzverstöße, diskriminierende Inhalte, Datenabflüsse oder die bewusste Manipulation von KI durch Dritte.

Insgesamt stellt der Kriterienkatalog ein umfassendes Regelwerk dar, das den verantwortungsvollen, rechtskonformen und sicheren Einsatz generativer KI in der Bundesverwaltung gewährleisten soll. Er richtet sich gleichermaßen an Leitungspersonal, IT-Verantwortliche und Fachabteilungen und soll für mehr Transparenz sowie Sicherheit bei der Nutzung einer sich rasant entwickelnden Technologie sorgen.

3. Fazit

Die Leitlinien für den Einsatz von KI in der Bundesverwaltung sowie der ergänzende Kriterienkatalog für generative KI bilden gemeinsam einen wichtigen Rahmen für den verantwortungsvollen und zielgerichteten Umgang mit KI-Technologien im öffentlichen Sektor. Sie bieten Orientierung bei der Entwicklung, Einführung und Anwendung von KI-Systemen und fördern dabei Transparenz, Nachvollziehbarkeit und ethische Vertretbarkeit. Die Leitlinien schaffen ein gemeinsames Verständnis für Chancen und Risiken von KI und stärken das Vertrauen in staatliches Handeln. Der Kriterienkatalog konkretisiert diese Grundsätze speziell für generative KI, indem er praxistaugliche Maßstäbe für Einsatzbereiche, Risikoabwägung und Entscheidungsprozesse definiert. Zusammen ermöglichen beide Instrumente eine systematische und vorausschauende Nutzung von KI in der Bundesverwaltung und tragen so dazu bei, Innovation mit gesellschaftlicher Verantwortung zu verbinden.

Gerne unterstützen wir Sie bei der rechtssicheren und verantwortungsvollen Umsetzung der Leitlinien und des Kriterienkatalogs im Rahmen von KI-Projekten.

Jason Komninos, LL.M.
Rechtsanwalt, Fachanwalt für Informationstechnologierecht
vCard

TOP-THEMA

Ende-zu-Ende-Verschlüsselung: Für Behörden keine standardmäßige Pflicht

Eine Bestandsaufnahme anhand der Entscheidung des OVG NRW vom 20.02.2025, Az. 16 B 288/23

Obwohl die Ende-zu-Ende-Verschlüsselung im elektronischen Verkehr als besonders sicher gilt, sind Behörden in Deutschland nicht gesetzlich verpflichtet, sie standardmäßig zu nutzen. Für die Hintergründe, warum das so ist und welche rechtlichen Rahmenbedingungen gelten, lohnt sich ein Blick in ein Verfahren, das vor den Verwaltungsgerichten in Nordrhein-Westfalen geführt wurde. Im Zentrum stehen die Fragen, inwieweit Behörden verpflichtet sind, technisch höchste Sicherheitsstandards wie Ende-zu-Ende-Verschlüsselung umzusetzen, und ob betroffene Personen hierauf einen durchsetzbaren Anspruch haben. Die Entscheidung zeigt exemplarisch, wie sich datenschutzrechtliche Anforderungen mit verwaltungspraktischen Realitäten überschneiden.

1. Was ist die Ende-zu-Ende-Verschlüsselung?

Ende-zu-Ende-Verschlüsselung im elektronischen Verkehr bedeutet, dass nur Sender und Empfänger den Inhalt einer Nachricht lesen können. Die Ende-zu-Ende-Verschlüsselung wird häufig im E-Mail-Verkehr, aber auch bei Chat-Messengern als technische Sicherheitsmaßnahme eingesetzt:

- Der Sender verschlüsselt die Nachricht mit einem Schlüssel, den nur er und der Empfänger kennen. Nur wer den Schlüssel hat, ist in der Lage, die Nachricht zu entschlüsseln. Selbst der E-Mail-Dienstanbieter hat keinen Zugriff auf den Inhalt einer E-Mail.

- Die Nachricht "reist" verschlüsselt durch das Internet und ist unterwegs nicht lesbar.

- Nur der Empfänger besitzt den passenden Schlüssel zum Entschlüsseln der Nachricht, der ihm das Lesen der Nachricht erlaubt.

Eine andere häufig implementierte Verschlüsselungstechnik ist die Transportverschlüsselung, auch TLS genannt. Hierbei wird die Verbindung zwischen dem Sender und dem Server des Empfängers verschlüsselt. Auf dem Server liegen die Nachrichten und Daten dann hingegen wieder unverschlüsselt. Das heißt, dass TLS nur die Verbindung schützt. Am

Beispiel einer E-Mail bedeutet das, dass die Verbindung zwischen E-Mail-Programm und Server des E-Mail-Providers verschlüsselt ist. Auf dem Server liegt die E-Mail aber meist im Klartext vor, sodass sie für Dritte zugänglich ist. Bei der Ende-zu-Ende-Verschlüsselung liegt die Verschlüsselung direkt auf dem Inhalt, sodass sie auch im Stadium des Speicherns auf dem Server geschützt ist.

2. Der Fall im Überblick

In einem verwaltungsgerichtlichen Eilverfahren über zwei Instanzen hatten die Gerichte zur Ende-zu-Ende-Verschlüsselung zu entscheiden.

Der Antragsteller, der beruflich mit explosiven Stoffen handelte, ließ sich in das Transparenzregister nach dem Geldwäschegesetz als Begünstigter der entsprechenden Sprengstoffunternehmen eintragen. Anschließend beantragte er die vollständige Beschränkung der Einsichtnahme, sodass ihn betreffende Angaben im Transparenzregister nicht eingesehen werden konnten. Er begründete dies mit seinem beruflichen Umgang mit Sprengstoff. Deshalb bestünde die Gefahr, dass er Opfer von Straftaten gegen das Leben werden könnte. Aus diesem Grund widersprach er, zusätzlich zu dieser Beschränkung, auch der Datenverarbeitung nach der Datenschutz-Grundverordnung (DSGVO) und machte die Einschränkung der Verarbeitung seiner Daten geltend. Dies solle für jedwede Form der Datenübertragung gelten, sowohl innerhalb des EDV-Systems der Antragsgegnerin als auch im Rahmen der Datenübermittlung an Dritte und an den Antragsteller selbst. Damit bezweckte der Antragsteller, dass die Übermittlung und Verarbeitung seiner personenbezogenen Daten durch die Antragsgegnerin, die registerführende Stelle, auch im Falle einer Kontaktaufnahme nur im Wege der Ende-zu-Ende Verschlüsselung erfolgen sollte. Eine einfache Transportverschlüsselung (TLS) reiche aus seiner Sicht nicht aus, da diese ein geringeres Schutzniveau als die Ende-zu-Ende-Verschlüsselung biete. Eine Nutzung seiner elektronischen Kontaktdaten zur Kommunikation sei ausdrücklich nicht erwünscht. Der Korrespondenz per Post stimmte der Antragsteller zu.

Da für die Eintragung der Beschränkung der Einsichtnahme die Verifizierung des Antragstellers mittels eines Ausweisdokuments notwendig war, versuchte die Antragsgegnerin diesen telefonisch zu erreichen. Hierauf reagierte der Antragsteller mit der Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung. Die Antragsgegnerin habe das Einschränkungsverlangen missachtet, weil sie versucht habe, ihn telefonisch zu kontaktieren.

Da die Antragsgegnerin die geforderte Unterlassungserklärung nicht abgab, beantragte der Antragsteller den Erlass einer einstweiligen Verfügung, weil er einen Anspruch auf die Ende-zu-Ende-Verschlüsselung habe. Diesen Anspruch leitete er aus Art. 18 Abs. 1 lit. d) i.V.m. Art. 21 Abs. 1, Art. 5 Abs. 1 lit. f) i.V.m. Art. 32 DSGVO ab.

Die Antragsgegnerin berief sich auf ihr mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstelltes Informationssicherheitskonzept, das einen hohen Sicherheitsstandard gewähre. Jedenfalls habe der Antragsteller keinen Anspruch auf eine Ende-zu-Ende-Verschlüsselung. Die von der Antragsgegnerin verwendete TLS-Verschlüsselung sei ausreichend und genüge den Anforderungen von Art. 32 DSGVO. Bei der Kommunikation mit anderen Behörden kämen sogar weitere Sicherheitsmaßnahmen zum Einsatz (Kommunikation über Sichere-Inter-Netzwerk-Architektur-Box und Client-Zertifikate). Ein Risiko, das zur Ergreifung höherer Sicherheitsmaßnahmen führe, bestünde im Falle des Antragstellers nicht.

3. Entscheidungen der Gerichte

Erstinstanzlich lehnte das Verwaltungsgericht Köln den Antrag des Antragstellers ab und versagte ihm damit den Anspruch auf die Ende-zu-Ende-Verschlüsselung (Beschluss vom 2. März 2023, Az. 13 L 1467/22). Diese Entscheidung hat das Oberverwaltungsgericht für das Land Nordrhein-Westfalen (OVG NRW) in der zweiten Instanz bestätigt (Beschluss vom 20. Februar 2025, Az. 16 B 288/23).

3.1 Anspruch auf ausschließliche Datenverarbeitung im Wege der Ende-zu-Ende Verschlüsslung

Das VG Köln stellte fest, dass ein Anspruch auf eine ausschließliche Datenverarbeitung im Wege der Ende-zu-Ende Verschlüsselung grundsätzlich aus der DSGVO abzuleiten sei. Demnach erkennt das Gericht einen subjektiven Anspruch hierauf an. Die konkrete Anspruchsgrundlage liege in Art. 32 DSGVO. Nach Art. 32 Abs. 1 DSGVO sei die Antragsgegnerin bei der Verarbeitung personenbezogener Daten verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.2 Auf die Risikoabwägung kommt es an

Trotz des grundsätzlichen Anspruchs nach Art. 32 DSGVO lehnte das VG Köln jedoch im vorliegenden Fall das Begehren des Antragstellers ab. Um die Geeignetheit einer Maßnahme zu ermitteln, müsse sie, gemessen am Risiko der Verarbeitung, ein angemessenes Schutzniveau bieten. Es sei daher zu ermitteln und festzustellen, wie groß die Risiken seien, die betroffenen Personen drohen könnten. Außerdem sei die Wahrscheinlichkeit eines Schadenseintritts zu berücksichtigen. Die konkrete Maßnahme müsse daher umso wirksamer ausgestaltet werden, je höher die drohenden Schäden ausfallen könnten. Die Angemessenheit des Schutzniveaus sei anhand des Risikos der Datenverarbeitung zu ermitteln.

Kurz gesagt: Maßgeblich ist die Risikoeinschätzung basierend auf dem Schutzbedarf der Daten.

Im konkreten Fall hatte die registerführende Behörde, entgegen dem Verlangen des Antragstellers, eine einfache Transportverschlüsselung für die elektronische Übermittlung der Daten innerhalb ihrer Systeme und gegenüber anderen Behörden genutzt. Das Gericht sah aber keine Anhaltspunkte dafür, dass eine über die Transportverschlüsselung hinausgehende Ende-zu-Ende-Verschlüsselung notwendig war. Aus den Entscheidungsgründen ergibt sich, dass der Antragsteller im vorliegenden Fall nicht umfassend und ausreichend dazu vorgetragen habe, dass ein besonderes Risiko bei der Verarbeitung seiner Daten vorliege, das eine Ende-zu-Ende-Verschlüsselung notwendig mache. Im Übrigen stellte das Gericht allgemein fest, dass die Datenübertragung bei der Antragsgegnerin stets unter TLS-Verschlüsselung und jedenfalls bei Kommunikation mit anderen staatlichen Stellen zusätzlich durch Client-Zertifikate oder die SINA-Box gesichert werde. Außerdem gehöre es zum allgemeinen Lebensrisiko, dass unbefugte Dritte Kenntnis von Inhalten der elektronischen Kommunikation nehmen könnten.

3.3 Bestätigung durch das OVG

Der Antragsteller ging gegen den Beschluss des Verwaltungsgerichts Köln vor und erhob Beschwerde vor dem OVG NRW. Diese hatte aber keinen Erfolg und wurde vom OVG zurückgewiesen. Das OVG schließt sich den Ausführungen der Vorinstanz zur Ende-zu-Ende-Verschlüsselung an. Es stellt fest, dass keine Anhaltspunkte für ein gesteigertes Risiko bestünden, dass der Antragsteller Opfer von Hackerangriffen werde, und sich deshalb kein erhöhtes Risiko für die Datenverarbeitung ableiten

lasse. Außerdem stellt sich das OVG auch im Hinblick auf die Verschlüsselung über TLS auf die Seite des VG Köln. Diese sei nicht die einzige Sicherheitsmaßnahme. Das TLS sei so ausgestaltet, dass sie vom Browser-Client zur Firewall der Antragsgegnerin reiche und damit gebe es keine Zwischenstation, auf der die Inhalte unverschlüsselt abgelegt wären. Außerdem sicherten die SINA-Box und Client-Zertifikate die Datenverarbeitungen hinreichend ab.

4. Tipps & Hinweise

Auch wenn die gerichtlichen Entscheidungen klar aussagen, dass eine Ende-zu-Ende-Verschlüsselung nicht standardmäßig gefordert werden kann, ist "zu viel" Datenschutz nie verkehrt. Dies gilt insbesondere mit Blick darauf, dass im behördlichen Alltag oft die Zeit fehlt, eine Risikoabwägung vorzunehmen, wie sicher Daten nun verarbeitet und übermittelt werden müssen. Art. 32 DSGVO zählt beispielhaft auf, wie personenbezogene Daten geschützt werden können. Darunter wird auch die Verschlüsselung genannt. Auch wenn keine spezifischen Anforderungen an die einzelnen Möglichkeiten gestellt werden, ist zu berücksichtigen, dass die Maßnahmen dem Stand der Technik entsprechen müssen. Insofern gewährleistet die Ende-zu-Ende-Verschlüsselung ein sehr hohes technisches Sicherheitsniveau. Allerdings erfordert ihre Implementierung eine sorgfältige Planung hinsichtlich Schlüsselmanagement, Benutzerfreundlichkeit und technischer Infrastruktur, um sowohl Sicherheit als auch praktische Anwendbarkeit zu gewährleisten. Auch die anfallenden Kosten, die nicht unerheblich sind, dürfen dabei nicht außer Acht gelassen werden.

Bei Datenverarbeitungen, die besonders sensible Daten betreffen, sind erhöhte Schutzmaßnahmen zu ergreifen. Dies betrifft insbesondere Daten besonderer Kategorien, wie etwa Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO. Höhere Sicherheitsmaßstäbe sollten allerdings auch bei der Verarbeitung der Daten von Kindern angelegt werden.

Schließlich sind aber nicht nur allein die Verschlüsselungsmaßnahmen als technische und organisatorische Maßnahmen relevant. Es kann schon viel durch Sensibilisierung und Awareness der Mitarbeiter für Datensicherheit erreicht werden.

Mirjam Kaiser
Rechtsanwältin
vCard

Arbeitsrecht

Diskriminierung von Teilzeitbeschäftigten bei tariflichen Überstundenzuschlägen

BAG, Urteil vom 5. Dezember (Az.: 8 AZR 370/20)

Kann in einer formalen Gleichbehandlung von Teilzeit- und Vollzeitbeschäftigten bei der Anwendung von sog. Auslösegrenzen für Überstundenzuschläge eine Diskriminierung liegen? Und wenn ja: Kann eine zur Sicherstellung der Gleichbehandlung erforderliche Ungleichbehandlung gerechtfertigt und notwendig sein, obwohl sich diese wiederum benachteiligend zulasten der Vollzeitbeschäftigten auswirken muss?

Mit diesen bereits paradox anmutenden Fragen hatte sich das Bundesarbeitsgericht (BAG) Ende des vergangenen Jahres mit Urteil vom 5. Dezember (Az.: 8 AZR 370/20) zu befassen und darauf erkannt, dass formal gleichbehandelnde Auslösegrenzen für Überstundenzuschläge unzulässig sein können; selbst dann, wenn sie in Tarifverträgen von Gewerkschaften und Arbeitgeberverbänden vereinbart und für angemessen befunden wurden.

Zur Problemstellung: Anwendung des Diskriminierungsverbots auf einheitliche Auslösegrenzen bei tarifvertraglichen Überstundenzuschlägen

In Teilzeit tätige Mitarbeiterinnen und Mitarbeiter (nachfolgend einheitlich "Mitarbeiter") dürfen gegenüber vergleichbaren Vollzeitbeschäftigten nicht benachteiligt werden. Es sei denn, dass sachliche Gründe eine unterschiedliche Behandlung rechtfertigen. Das Diskriminierungsverbot zugunsten von in Teilzeit beschäftigten Arbeitnehmern ist in § 4 Abs. 1 Satz 1 Teilzeit- und Befristungsgesetz (TzBfG) ausdrücklich niedergelegt.

Aber stellt es überhaupt eine Ungleichbehandlung dar, wenn eine in einem Tarifvertrag geregelte Auslösegrenze für Überstundenzuschläge alle Mitarbeiter einheitlich behandelt, d.h. die Zuschläge stets erst dann geschuldet sind, wenn die vertragliche Arbeitszeit eines Vollzeitbeschäftigten überschritten wird?

Mit dieser Frage hatte sich das *BAG* in seiner Entscheidung vom 5. Dezember (Az.: 8 AZR 370/20) konkret zu befassen.

Zum Urteil des *BAG* vom 5. Dezember (Az.: 8 AZR 370/20)

Bei der Entscheidung des *BAG* vom 5. Dezember (Az.: 8 AZR 370/20) ging es um Pflegekräfte eines großen ambulanten Dialyseanbieters.

Die Klägerin war in Teilzeit im Umfang von 40% einer Vollzeitkraft tätig. Der auf das Arbeitsverhältnis anwendbare Haus-Tarifvertrag sah Überstundenzuschläge vor, die aber erst bei Überschreiten der wöchentlichen Arbeitszeit eines vollzeitbeschäftigten Mitarbeiters (38,5 Stunden) zu zahlen waren.

Wie bereits der *Gerichtshof der Europäischen Union* (EuGH), dem die streitentscheidende Rechtfrage zur Vorabentscheidung vorgelegt worden war (vgl. *EuGH*, Urteil vom 29. Juli 2024 – C-184/22 und C-185/22 – *KfH Kuratorium für Dialyse und Nierentransplantation*; s. zuvor bereits: *EuGH*, Urteil vom 19. Oktober 2023 – C-660/20 – *Lufthansa CityLine*) sah das BAG eine unzulässige Ungleichbehandlung darin, dass die im Tarifvertrag geregelte Auslösegrenze für Überstundenzuschläge Voll- und Teilzeitkräfte formal gleichbehandelte.

Es ist nach dem *BAG* damit rechtlich zu beanstanden, wenn ein in Teilzeit beschäftigter Mitarbeiter bei Überschreiten seiner individuellen Arbeitszeit Überstunden leisten muss, ohne in den Genuss von Zuschlägen zu kommen, während einer vergleichbaren Vollzeitkraft bereits ab der ersten Überstunde Zuschläge gezahlt werden. Hierin läge eine Ungleichbehandlung der Teilzeitkraft im Sinne des Diskriminierungsverbots aus § 4 Abs. 1 Satz 1 TzBfG. Hieran sind auch die Tarifvertragsparteien bei Abschluss von Tarifverträgen gebunden.

Die in der formalen Gleichbehandlung von Teilzeit- und Vollzeitkräften liegende Ungleichbehandlung bei der Auslösegrenze für Überstundenzuschläge sei – so das *BAG* – auch nicht aus sachlichen Gründen gerechtfertigt: Keinen sachlichen Grund für die Ungleichbehandlung erkannte es darin, dass in der Folge Teilzeitbeschäftigte bereits Überstundenzuschläge erhalten, während ihre in Vollzeit beschäftigten Arbeitskollegen – bei identischer Stundenbelastung – noch auf Basis der Grundvergütung arbeiten müssen.

Quintessenz der Entscheidung

Es ist nach dem BAG folglich regelmäßig unzulässig, wenn Teilzeitbeschäftigte erst dann Überstundenzuschläge erhalten, wenn sie im jeweiligen Referenzzeitraum die maßgebliche Arbeitszeit eines in Vollzeit beschäftigten Mitarbeiters überschreiten. Dies, obwohl sich eine auf das Teilzeit-Arbeitszeitniveau angepasste Auslösegrenze benachteiligend zulasten der in Vollzeit beschäftigten Mitarbeiter auswirken muss: Teilzeitbeschäftige erhalten für ihre Mehrarbeit bereits Überstundenschläge, während sich ihre in Vollzeit beschäftigten Arbeitskollegen für die identische Arbeit noch mit ihrer Grundvergütung begnügen müssen. Kann das aber richtig sein?

Mehr noch: Das *BAG* hat in der formal gleichbehandelnden tarifvertraglichen (!) Auslösegrenze ebenfalls eine entschädigungspflichtige mittelbare Diskriminierung von in Teilzeit beschäftigten Mitarbeiterinnen wegen des Geschlechts im Sinne der §§ 15 Abs. 2, 7 Abs. 1 und 3 Abs. 2 des Allgemeinen Gleichbehandlungsgesetzes (AGG) erkannt, wenn in der Gruppe der in Teilzeit beschäftigten Mitarbeiter "signifikant" (Was auch immer dies bedeutet?) mehr Frauen als Männer vertreten sind.

Dieses Urteil hat enorme Sprengkraft, weil es sowohl Grundsatzfragen zur innerbetrieblichen Lohngerechtigkeit als auch zur Reichweite der grundrechtlich geschützten Tarifautonomie (Art. 9 Abs. 3 GG) aufwirft. Denn: Warum soll es eigentlich unzulässig sein, wenn Tarifvertragsparteien es für "fair und angemessen" ansehen, dass Zuschläge für Überstunden erst nach Überschreiten der Arbeitszeit eines Vollzeitbeschäftigten (38,5 Stunden) geschuldet sind?

Folgen für die Praxis

Man kann die Entscheidung des BAG mit guten Argumenten für falsch halten. Denn: Es muss nicht einleuchten, warum ein in Teilzeit beschäftigter Arbeitnehmer bereits Zuschläge für Überstunden erhalten soll, während sein in Vollzeit tätiger Arbeitskollege noch "regulär" arbeiten muss. Oder provokativ gefragt: Gibt es zukünftig nur noch Teilzeit?

Die Praxis muss sich auf die Rechtsprechung des BAG gleichwohl einstellen: Verstößt eine tarifvertragliche Regelung gegen ein Diskriminierungsverbot, so nimmt das BAG in der Rechtsfolge eine sog. "Anpassung nach oben" vor: Teilzeitbeschäftigte haben folglich bereits ab ihrer ersten Überstunde Anspruch auf Zuschläge, selbst wenn der Tarifvertrag dies abweichend regelt.

Ausnahmsweise kann eine formal gleichbehandelnde tarifvertragliche Zuschlagsregelung jedoch wirksam sein, wenn im Tarifvertrag hinreichend deutlich zum Ausdruck kommt, dass die Zuschläge gerade deshalb gezahlt werden sollen, um die besonderen Belastungen zu entschädigen, die davon ausgehen, dass über die reguläre Stundenanzahl eines Vollzeitbeschäftigten hinaus gearbeitet werden muss. Dieser Anforderung werden allerdings die wenigsten Tarifverträge genügen. Selbst aber, wenn ein Tarifvertrag dies hergeben sollte, wird das BAG die "Besserstellung" der Vollzeitbeschäftigen kritisch prüfen und danach fragen, ob sich die vertragliche Tätigkeit überhaupt als physisch oder psychisch besonders belastend darstellt und damit als Grund für die Ungleichbehandlung (bzw. formale Gleichbehandlung) trägt.

Michael Riedel
Rechtsanwalt, Fachanwalt für Arbeitsrecht
vCard

Dr. Martin Kalf, LL.M. (Edinburgh)
Rechtsanwalt, Fachanwalt für Arbeitsrecht
vCard

Energierecht

KSpTG: Neue Chancen bei CO2-Speicherung und Infrastruktur

Die Bundesregierung hat am 6. August ihren Kabinettsentwurf zur Änderung des Kohlendioxid-Speicherungsgesetzes verabschiedet, der den Rechtsrahmen für CO2-Speicherstätten und Leitungen erneuert. Das Gesetz wird nun zum Kohlendioxid-Speicherung und Transport Gesetz (KSpTG). Ziel sei es, die Technologien zur CO2-Abscheidung (CCS) und -Verwertung (CCU) für Industrieemissionen voranzubringen alsein weiterer Baustein zur Erreichung der Klimaziele.

Was bedeutet das für die öffentliche Hand?

1. Fördermittel für Infrastrukturprojekte

Die bisherige Zulassung von Speichervorhaben zu reinen Erforschungs-, Erprobungs- und Demonstrationszwecken wird im KSpTG für alle kommerziellen Verwender geöffnet. Diese werden vor allem Emittenten mit schwer vermeidbaren Emissionen sein, z.B. Müllverbrennungsanlagen, Teile der Chemieindustrie und der Zement- und Kalksektor. Speziell für diese Gruppe von Emittenten wurde durch die Bundesförderung Industrie und Klimaschutz (BIK) ein bis 2030 laufender Fördertopf eingerichtet, welcher für dezidierte CCS-Infrastruktur- und Speicherprojekte bis zu EUR 25 Mio. pro Projekt bereitstellt.

2. Gaskraftwerke bleiben relevant

Kohlekraftwerke werden im KSpTG vom Anschluss an das CO2-Leitungsnetz ausdrücklich ausgeschlossen, Gaskraftwerke jedoch nicht. Damit wird ihre Rolle als flexible Reserve im Strommix gestärkt. CCS kann helfen, die konventionelle Gasverstromung bis zum Übergang zu Wasserstoff deutlich emissionsärmer zu gestalten.

3. Mitgestaltung bei Speicherstandorten

Das Gesetz erlaubt künftig die CO2-Speicherung nicht nur offshore, sondern auch auf dem Festland, um die weiten Transportwege zur Küste zu vermeiden – sofern die Bundesländer aktiv zustimmen. Dies wird aber maßgeblich von der Zustimmung der lokalen Kommunen abhängen, die vielerorts CCS-Landspeicherstätten mit Skepsis begegnen. Dabei werden dem Bau und Betrieb von Wasserstoffleitungen, Windanlagen und deren Anbindungsleitungen Vorrang gewährt sowie umfangreiche Meeresschutzgebiete von der Einlagerung ausgeschlossen.

4. Planungs- und Genehmigungsbeschleunigung beim Leitungsausbau

Das KSpTG regelt nun uneingeschränkt die Genehmigung und den Betrieb aller Arten von Kohlendioxidleitungen. Um das Planungs- und Genehmigungsverfahren sowohl für Behörden als auch für Betreiber einfacher zu machen, verwies das alte KSpG schon an vielen Stellen auf wesentliche Verfahrensbeschleuniger aus dem Energiewirtschaftsgesetz (EnWG), die sich beim Errichten von Gasleitungen bewährt haben. Die Bezugspunkte werden im neuen KSpTG ausgeweitet und an den zwischenzeitlichen Neuerungen im EnWG angepasst. Bestehende Gas-oder Wasserstoffleitungen können künftig ohne neues Planfeststellungsverfahren auf den Transport von Kohlendioxid umgestellt werden.

5. Vorrang für CO2-Infrastruktur

Für die Abwägung im Rahmen des Planfeststellungsverfahrens gilt nun, dass der Bau von Kohlendioxidleitungen im überragenden öffentlichen Interesse liegt und behördlichen Vorrang bei der Bearbeitung erhält. Im Rahmen der Abwägung haben die Behörden zu berücksichtigen, dass Kohlendioxidleitungen dazu beitragen, Emissionen in Deutschland dauerhaft zu mindern. Neue Ergänzung ist zudem, dass in Fällen der Parallelverlegung neben schon bestehenden Wasserstoffleitungen eine widerlegliche Vermutung dafür besteht, dass keine zusätzliche Beeinträchtigung anderer Belange vorliegt.

Fazit

Das KSpTG schafft neue Spielräume für kommunale und landespolitische Akteure, um aktiv zur Dekarbonisierung beizutragen. Wer frühzeitig prüft, ob lokale Infrastruktur, Flächen oder kommunale Unternehmen für CCS/CCU geeignet sind, kann von Fördermitteln und beschleunigten Verfahren profitieren.

Dr. Malaika Ahlers
Rechtsanwältin
vCard

Anton Buro

Rechtsanwalt
vCard

Prozessführung

Prozessführung der öffentlichen Hand und der Umgang mit Informationsbegehren von Prozessgegnern

Wenn die öffentliche Hand gerichtliche Streitigkeiten führt, sieht sie sich besonderen Herausforderungen konfrontiert.

Prozessgegner versuchen mitunter, tatsächliche oder behauptete Informationsdefizite durch Anträge nach dem Informationsfreiheitsgesetz (IFG) oder dem Umweltinformationsgesetz (UIG) zu kompensieren. Ziel ist häufig der Zugang zu internen behördlichen Unterlagen, die insbesondere im Zivilprozess nicht freiwillig offengelegt würden. So können Prozessgegner versuchen, den dort geltenden Beibringungsgrundsatz zu ihrem Vorteil auszuhebeln. Nach dem Beibringungsgrundsatz hat bekanntermaßen jede Prozesspartei die für ihren Anspruch oder ihre Verteidigung entscheidungsrelevanten Tatsachen selbst vorzutragen und die entsprechenden Beweismittel beizubringen.

1. Informationszugangsgesetze als Instrument der Prozessvorbereitung

Das IFG gewährt jedermann einen voraussetzungslosen Anspruch auf Zugang zu amtlichen Informationen bei Bundesbehörden; entsprechende Regelungen bestehen auf Landesebene. Das UIG regelt den Zugang zu Umweltinformationen und gilt auch für private Stellen mit öffentlichen Umweltaufgaben. Beide Gesetze enthalten Ausschlusstatbestände, etwa zum Schutz personenbezogener Daten, von Betriebs- und Geschäftsgeheimnissen, laufenden Gerichtsverfahren oder der öffentlichen Sicherheit.

Die Rechtsprechung legt diese Ausnahmen jedoch restriktiv aus. Die Darlegungslast für deren Vorliegen liegt bei der informationspflichtigen Behörde. Dies kann dazu führen, dass die öffentliche Hand zur Herausgabe prozessrelevanter Informationen verpflichtet wird – und zwar gegenüber einem Gegner, dem sie gleichzeitig im Zivilprozess gegenübersteht.

2. Zivilprozessuale Instrumente und deren Grenzen

2. Zivilprozessuale Instrumente und deren Grenzen

Die Zivilprozessordnung stellt mit § 142 ZPO (gerichtliche Anordnung der Urkundenvorlegung) und § 421 ZPO (Vorlegungspflicht des Gegners) eigene Mechanismen zur Verfügung, um Unterlagen zu erlangen. Die Anforderungen sind jedoch hoch:

- § 142 ZPO: Die Anordnung steht im Ermessen des Gerichts. Es muss ein schlüssiger, konkreter Tatsachenvortrag erfolgen. Eine Beweiserhebung „ins Blaue hinein" ist unzulässig. Zudem sind Geheimnisschutz und Persönlichkeitsrechte zu berücksichtigen.
- § 421 ZPO: Der Antragsteller muss darlegen, dass sich die Urkunde im Besitz des Gegners befindet und ein materiell-rechtlicher Anspruch auf Vorlage besteht oder der Gegner sich auf die Urkunde bezogen hat.

In der Praxis sind diese Hürden oft schwer zu überwinden. Daher versuchen Prozessgegner, über IFG/UIG-Anträge Informationen zu erlangen, die sie auf zivilprozessualem Wege nicht erhalten würden.

3. Prozessuale Risiken für die öffentliche Hand

Die strategische Nutzung von Informationszugangsgesetzen kann zu erheblichen Nachteilen führen:

- Verwendung von Umweltgutachten aus Genehmigungsverfahren
- Einsicht in interne Vermerke, Rechtsgutachten oder Vergabeunterlagen
- Umgehung gerichtlicher Schutzmechanismen durch parallele Informationsanträge
- Verzögerung und Belastung der Verwaltung durch zusätzliche Verfahren

Die Offenlegung kann nicht nur die prozessuale Position schwächen, sondern auch über den konkreten Rechtsstreit hinausgehende Folgen haben.

4. Handlungsempfehlungen

Für die öffentliche Hand ergeben sich daraus folgende Erfordernisse:

- Sorgfältige Prüfung im Informationszugangsverfahren, insbesondere der Ausschlusstatbestände
- Strategische Prozessführung, um Nachteile durch Offenlegung zu vermeiden
- Verwaltungsprozessuale Gegenmaßnahmen bei unzulässigen Informationsbegehren
- Enge Abstimmung zwischen Verwaltungs- und Zivilprozessführung

Zivilgerichtliche Verfahren, in denen Informationsbegehren nach dem IFG oder dem UIG eine Rolle spielen, stellen öffentliche Stellen zunehmend vor komplexe rechtliche und taktische Herausforderungen. Gerade in Zivilprozessen, in denen der Beibringungsgrundsatz gilt, können solche Begehren gezielt eingesetzt werden, um die öffentliche Hand unter Druck zu setzen oder strategisch zu benachteiligen.

Die zivilprozessualen Anforderungen und Risiken, die sich aus solchen Konstellationen ergeben, erfordern eine sorgfältige rechtliche Einordnung und strategische Vorgehensweise. Dazu zählen insbesondere:

- Die Abgrenzung zwischen zulässiger Beweiserhebung und unzulässigem Ausforschungsbeweis
- Die strategische Nutzung von Schutzmechanismen, etwa durch Anträge nach § 273a ZPO zur Sicherung vertraulicher Informationen
- Die Abwehr von Vorlegungsanträgen nach §§ 142, 421 ZPO, wenn die Voraussetzungen nicht erfüllt sind
- Die Koordination mit verwaltungsrechtlichen Verfahren, etwa bei parallelen IFG/UIG-Anträgen

Behörden und Ministerien sehen sich im Zivilprozess – ebenso wie in anderen Streitigkeiten – besonderen Anforderungen gegenüber, etwa im Hinblick auf prozessuale Taktiken, interne Abstimmungsprozesse und die Einhaltung verwaltungsrechtlicher Vorgaben, insbesondere:

- Präventive Beratung zur Dokumentation und Schutzwürdigkeit potenziell prozessrelevanter Informationen
- Verteidigung gegen strategisch motivierte Auskunftsbegehren, insbesondere bei paralleler zivilprozessualer Betroffenheit
- Prozessführung in komplexen Verfahren, in denen IFG/UIG-Informationen als Beweismittel eingesetzt werden sollen
- Interdisziplinäre Koordination zwischen Zivilprozessführung, Informationsfreiheitsrecht und behördlicher Kommunikation

Die frühzeitige Identifikation von Risiken und die gezielte Wahrung der Interessen der öffentlichen Hand setzen ein vertieftes Verständnis der zivilprozessualen Mechanismen sowie Erfahrung in der Zusammenarbeit mit öffentlichen Auftraggebern voraus.

Dr. Michael Späthe, LL.M.
Rechtsanwalt
vCard

Zur Newsletter Anmeldung

E-Mail weiterleiten

Hinweis: Wenn Sie künftig keine Informationen erhalten möchten, können Sie sich jederzeit abmelden.

Impressum

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH

Ganghoferstraße 33, 80339 München

AG München, HR B 155350/USt.-Idnr: DE-811218811

Tel.: +49 89 35065-0, Fax: +49 89 35065-123 | E-Mail: munich@advant-beiten.com

Hier finden Sie unser vollständiges Impressum: www.advant-beiten.com/impressum und unsere Datenschutzerklärung: www.advant-beiten.com/datenschutz