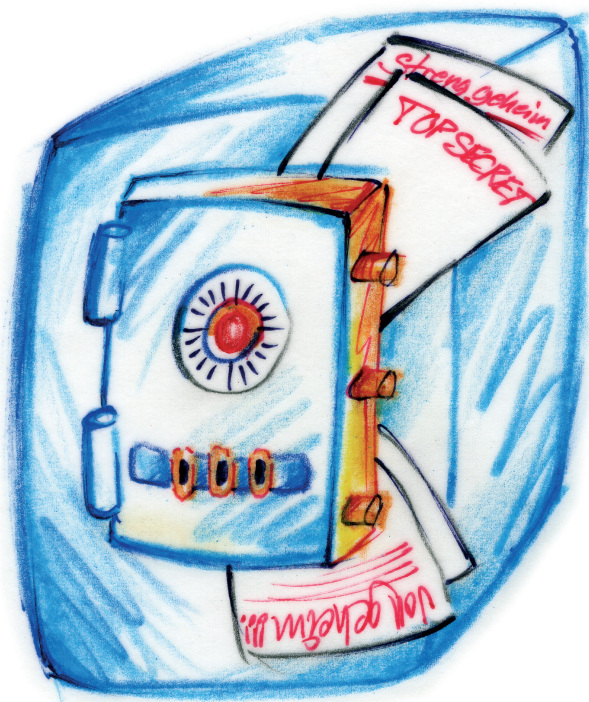


Datenschutzmerkblatt

Informationen für Beschäftigte des KIT

DATENSCHUTZ BETRIFFT UNS ALLE!



Sehr geehrte Mitarbeiterin, sehr geehrter Mitarbeiter,

im Zuge der fortschreitenden Digitalisierung personenbezogener Daten, immer komplexer werdender IT-Infrastrukturen und der zunehmenden Vernetzung von gespeicherten Daten ist Datenschutz zu einem unverzichtbaren und festen Bestandteil unseres Handelns geworden und nimmt in unserer Gesellschaft einen hohen Stellenwert ein.

Der richtige Umgang mit personenbezogenen Daten stellt auch für das Karlsruher Institut für Technologie (KIT) ein wichtiges und zentrales Anliegen dar.

Mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) wurde das Datenschutzrecht EU-weit vereinheitlicht. Die Verordnung findet direkte Anwendung und muss nicht in nationales Recht umgesetzt werden. Die nationalen Gesetzgeber wurden allerdings ermächtigt, einzelne Regelungen der DS-GVO durch eigene Regelungen zum Datenschutz zu konkretisieren und zu ergänzen. Hiervon hat der deutsche Gesetzgeber Gebrauch gemacht, sodass für das KIT ab dem 21. Juni 2018 neben der DS-GVO das Landesdatenschutzgesetz (LD SG) für Baden-Württemberg Anwendung findet.

Wir möchten Ihnen diese Informationsbroschüre an die Hand geben, um Ihnen den richtigen Umgang mit personenbezogenen Daten an Ihrer neuen Arbeitsstätte zu erleichtern. In diesem Merkblatt finden Sie Informationen zu den Grundbegriffen und Grundprinzipien des Datenschutzes und an wen Sie sich bei Fragen wenden können. Gleichzeitig erfahren Sie hier, wie Sie selbst durch einfache Vorkehrungen aktiv zum Datenschutz beitragen können.

Ihre Datenschutzbeauftragte des KIT

Allgemeine Informationen

ZWECK DES DATENSCHUTZES

Jeder Mensch hat das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Dieses Recht auf informationelle Selbstbestimmung (BVerfG, Urteil vom 15.12.1983, BVerfGE 65,1) stellt eine besondere Ausprägung des im Grundgesetz verankerten allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar.

Zweck des Datenschutzes ist es, die einzelne Person davor zu schützen, in ihrem Persönlichkeitsrecht – dem Recht auf informationelle Selbstbestimmung – und damit in ihrem Grundrecht verletzt zu werden.

IHR ARBEITSPLATZ

Im Rahmen Ihrer Tätigkeit am KIT werden Sie in der Regel mit personenbezogenen Daten in Berührung kommen.

Arbeitsplatzrechner und auch andere Geräte mit moderner Informationstechnik sowie viele zur Verfügung gestellte Softwarepakete und Programme ermöglichen Ihnen die elektronische, d. h. die automatisierte Verarbeitung von personenbezogenen Daten.



Nach der DS-GVO unterliegt allerdings nicht nur die automatisierte Datenverarbeitung den datenschutzrechtlichen Vorschriften. Daten, die in einem Dateisystem, d. h. in einer nach bestimmten Kriterien strukturierten Sammlung personenbezogener Daten wie beispielsweise Akten in der Registratur, gespeichert werden, unterliegen ebenfalls den datenschutzrechtlichen Vorschriften.

Da durch diese Verarbeitungen eine Verletzung des allgemeinen Persönlichkeitsrechts der Betroffenen möglich ist, ist stets größte Sorgfalt im Umgang mit personenbezogenen Daten geboten.

PERSONENBEZOGENE DATEN

Die Frage nach der Zulässigkeit der Verarbeitung von Daten stellt sich aus datenschutzrechtlicher Sicht immer nur dann, wenn es um personenbezogene Daten geht.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standorten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DS-GVO).

Der Begriff „personenbezogen“ ist demnach weit zu fassen. Es reicht bereits aus, wenn anhand einer vorliegenden Angabe oder aus der Gesamtheit mehrerer Einzelangaben eine Person identifiziert werden kann.

Beispiele für personenbezogene Daten sind:

- Name, Vorname
- Anschrift
- Alter
- Geburtsdatum
- Familienstand
- Telefonnummer
- E-Mail-Adresse
- Matrikelnummer
- Personalnummer
- Urlaubszeiten
- Gesundheitsdaten
- Angaben über die Einkommens- oder Vermögensverhältnisse
- Daten über die Zugehörigkeit zu politischen, kirchlichen oder anderen gesellschaftlichen Institutionen



GESETZLICHE REGELUNGEN

Bei jeder Verarbeitung personenbezogener Daten von Kolleginnen und Kollegen, Studierenden, Partnerinnen und Partnern im wissenschaftlichen Umfeld oder von anderen Personen sind die datenschutzrechtlichen Vorschriften zu beachten.

Unter Verarbeitung ist dabei jeder Vorgang von der Erhebung personenbezogener Daten über die Speicherung, Veränderung oder anderweitige Nutzung bis zur Offenlegung durch Übermittlung und Löschung zu verstehen.

Die bestehenden Rechtsvorschriften sollen Klarheit schaffen:

- ➔ Klarheit für Sie, wenn Sie Daten verarbeiten; Sie wissen, was Sie dürfen und welche Pflichten Sie haben.
- ➔ Klarheit für Sie als betroffene Person; Sie wissen, was Sie hinnehmen müssen und welche Rechte Sie haben.

Die für Sie geltenden wichtigsten Vorschriften in der jeweils gültigen Fassung sind unter anderem:

- EU-Datenschutz-Grundverordnung (DS-GVO)
- Landesdatenschutzgesetz (LDSG)
- Landeshochschulgesetz (LHG)

WAHRUNG DES DATENGEHEIMNISSES

Nach § 3 Abs. 2 LDSG sind Sie zur Wahrung des Datengeheimnisses verpflichtet:

„Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“

GRUNDSÄTZE DES DATENSCHUTZES

Die folgenden Grundsätze stellen die Grundregeln dar, die Sie bei jeder Verarbeitung von personenbezogenen Daten beachten müssen.

■ **Rechtmäßigkeit der Verarbeitung**

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn sie mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen zulässigen Rechtsgrundlage erfolgt.

Beispiel: Bewerberinnen und Bewerber um einen Studienplatz müssen für die Zulassung verschiedene personenbezogene Daten angeben. Die gesetzliche Grundlage bildet hier das baden-württembergische Landeshochschulgesetz i.V.m. der Hochschul-Datenschutzverordnung.

■ **Verarbeitung nach Treu und Glauben**

Hierunter ist die allgemeine Verpflichtung zur Fairness und zur Rücksichtnahme auf die Interessen und Erwartungen der betroffenen Person im Zusammenhang mit der Verarbeitung von personenbezogenen Daten zu verstehen.

■ **Transparenz**

Eine besondere Ausprägung des Grundsatzes der Verarbeitung nach Treu und Glauben stellt der Grundsatz der Transparenz dar. Die betroffene Person muss nachvollziehen können, ob, von wem und zu welchem Zweck ihre personenbezogenen Daten verarbeitet werden.

Hierzu ist es erforderlich, dass die betroffene Person Informationen zur Verarbeitung der personenbezogenen Daten erhält. Diese Informationen müssen präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sein.

Beispiel: Für die freiwillige Teilnahme an einer wissenschaftlichen Studie benötigt das mit der Durchführung der Studie beauftragte Institut von Ihnen eine Einwilligungserklärung. Aus dem Einwilligungstext muss dabei klar und

unmissverständlich hervorgehen, in welche Form der Verarbeitung Ihrer personenbezogenen Daten Sie einwilligen. Weitere wesentliche Informationen über die Verarbeitung Ihrer personenbezogenen Daten enthalten die zugehörigen Informationen zum Datenschutz (Datenschutzerklärung).

■ Zweckbindung

Personenbezogene Daten dürfen nur für die zur Aufgabenerfüllung festgelegten Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Beispiel: Sie haben im Rahmen einer Bedarfsermittlung von Kinderbetreuungsplätzen Ihre Kontaktdaten bei der zuständigen Abteilung angegeben, um über den neusten Stand informiert zu werden. Diese Daten dürfen nur für diesen Zweck verarbeitet und nicht für einen anderen Zweck wie z. B. zur Bewerbung des geplanten Weiterbildungskurses „Beruf und Familie vereinbaren“ verwendet werden.

■ Datenminimierung (Gebot der Erforderlichkeit)

Personenbezogene Daten dürfen nur verarbeitet werden, wenn dies zur Aufgabenerfüllung zwingend erforderlich ist und die Verarbeitung in einem angemessenen Verhältnis zum verfolgten Zweck steht.

Die Datenerhebung muss auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Sollten Daten nur nützlich oder hilfreich sein, liegt keine Erforderlichkeit vor.

Beispiel 1: Für die Aufgabenerfüllung am Arbeitsplatz ist es nicht erforderlich, dass alle Mitarbeiterinnen und Mitarbeiter aus einer Abteilung gegenseitig das Geburtsdatum kennen. Es ist damit nicht zulässig, eine Geburtsliste in der Abteilung allgemein zur Verfügung zu stellen.

Beispiel 2: Im Rahmen einer wissenschaftlichen Studie ist es für den konkreten Zweck dieses Forschungsprojektes nicht immer erforderlich, die Adressdaten der Probandinnen und Probanden zu erheben.

■ **Richtigkeit der Datenverarbeitung**

Die verarbeiteten personenbezogenen Daten müssen sachlich richtig sein und, soweit dies für die Verarbeitung erforderlich ist, aktualisiert werden. Soweit die Daten im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sind diese unverzüglich zu löschen oder zu berichtigen.

Beispiel: Hat sich aufgrund von Heirat Ihr Nachname geändert, muss im Personalverwaltungssystem der neue Name gespeichert werden. Andernfalls wäre die o. g. Angabe falsch.

■ **Speicherbegrenzung (zeitliche Datensparsamkeit)**

Daten, die die Identifizierung einer Person ermöglichen, dürfen nur so lange gespeichert werden, wie dies für die Zweckerreichung notwendig ist. Die Speicherdauer ist dabei auf das unbedingt erforderliche Mindestmaß zu beschränken.

Beispiel: Für die Aufbewahrung von Rechnungsunterlagen gelten bestimmte Aufbewahrungsfristen nach Handelsgesetzbuch (HGB). Nach Ablauf solcher Fristen sind die Unterlagen zu vernichten und gespeicherte Daten zu löschen.

Für Verarbeitungen beispielsweise zu wissenschaftlichen Forschungszwecken dürfen personenbezogene Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen länger gespeichert werden.

■ **Integrität und Vertraulichkeit**

Personenbezogene Daten sollen so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen.

Sie selbst können bei Ihrer täglichen Arbeit mit bereits wenigen Vorkehrungen zu einem sicherheitsbewussten Verhalten im Umgang mit personenbezogenen Daten beitragen.

Näheres hierzu erfahren Sie unter „Praktische Hinweise für den Arbeitsplatz“.

IHRE RECHTE ALS BETROFFENE PERSON

Nach der DS-GVO haben Sie gegenüber dem KIT folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

- Recht auf Information
- Recht auf Auskunft
- Recht auf Berichtigung und Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Widerspruch gegen die Verarbeitung (einzelfallabhängig)
- Recht auf Datenübertragbarkeit (einzelfallabhängig)
- Beschwerderecht bei der Aufsichtsbehörde

Bitte bedenken Sie dabei auch:

Die Rechte, die Sie als betroffene Person haben, stellen gleichzeitig auch Pflichten dar, sobald Sie selbst personenbezogene Daten im KIT verarbeiten. Insbesondere ist hierbei die Informationspflicht zu beachten.



Praktische Hinweise für den Arbeitsplatz

*Was kann ich selbst tun?
Was darf ich auf keinen Fall tun?*

Wichtigster Grundsatz bei der Nutzung der Informations- und Kommunikationstechnik sowie der Infrastruktur für digitale Informationsverarbeitung muss ein sicherheitsbewusstes Verhalten sein.

Nachfolgend finden Sie eine Auswahl von Empfehlungen und Verhaltensregeln im Zusammenhang mit der Verarbeitung personenbezogener Daten am KIT. Diese sollen Ihnen eine erste Orientierung geben. Bei vertieften Fragen wenden Sie sich bitte an die Stabsstelle Datenschutz (DSB).

Anfragen zu Personen

Geben Sie auf Anfragen – sei es in telefonischer Form oder per unverschlüsselter E-Mail – keine Daten heraus, bevor Sie nicht die Rechtmäßigkeit zuvor kritisch geprüft haben. Verweisen Sie daher grundsätzlich darauf, dass nur schriftliche Anfragen (auch Fax) beantwortet werden können.

Bei Anfragen von Ermittlungsbehörden dürfen Auskünfte nur über die Dienstleistungseinheit RECHT erfolgen. Bei Anfragen von anderen Behörden kontaktieren Sie bitte die Stabsstelle Datenschutz (DSB).

Personaldaten

Personenbezogene Daten der Beschäftigten dürfen nur verarbeitet werden, wenn dies im Zusammenhang mit der Begründung, Durchführung und Beendigung von Arbeitsverhältnissen oder zu Zwecken innerbetrieblicher Personalplanung erforderlich ist oder wenn es durch eine Rechtsvorschrift, durch einen Tarifvertrag oder durch eine Dienstvereinbarung vorgesehen ist. Zugang zu den Personaldaten dürfen nur Beschäftigte haben, für deren Aufgabenerfüllung dies erforderlich ist. Am KIT ist für Personalaktendaten grundsätzlich die Dienstleistungseinheit PSE (Personalservice) zuständig.

Daten von Studierenden

Veröffentlichen Sie keine Matrikelnummern im Internet, also auch keine Gruppeneinteilungen oder Prüfungstermine und vor allem keine Notenlisten mit Matrikelnummern. Veröffentlichen Sie Daten von Studierenden wie z. B. das Thema der Abschlussarbeit im Internet nur mit deren Einwilligung.

Schutzvorkehrungen im Büro

Schließen Sie Ihr Büro auch bei kurzer Abwesenheit grundsätzlich ab. Bewahren Sie herumliegende Unterlagen gerade bei Publikumsverkehr so auf, dass sie nicht einsehbar sind. Benutzen Sie abschließbare Schränke und halten Sie diese bei vertrauenswürdigen Daten auch verschlossen.

Entsorgungsangebote des KIT

Nutzen Sie die verschiedenen Möglichkeiten am KIT zur Entsorgung von vertrauenswürdigen Schriftgut und von datenschutzrechtlichem Material. Zuständig für die Entsorgung und auch für Fragen rund um die Abfallentsorgung ist die Abfallwirtschaftszentrale (erreichbar unter der Tel.-Nr. 608-22222).

Recht am eigenen Bild

Veröffentlichen Sie Bilder von Beschäftigten sowohl im Internet als auch im Intranet oder auf Papier grundsätzlich nur mit deren Einwilligung. In Zweifelsfällen kontaktieren Sie die Stabsstelle Datenschutz (DSB).

Versand von E-Mails an mehrere Empfänger

Verwenden Sie beim Versand von E-Mails an mehrere Empfänger die BCC-Funktion Ihres E-Mail-Programms, damit nicht alle Empfänger die Adressen der anderen sehen.

Unverschlüsselte elektronische Post ist wie eine Postkarte

Beim Versand unverschlüsselter E-Mails besteht die Gefahr, dass die Nachricht auf dem Weg vom Absender zum Empfänger von beliebig

vielen Personen gelesen oder sogar verändert wird. Personenbezogene Daten oder andere schutzwürdige Informationen dürfen auf diesem Weg nicht unverschlüsselt versandt werden. Am KIT besteht die Möglichkeit, verschlüsselte E-Mails zu versenden und zu empfangen und diese zu signieren.

Bitte bedenken Sie, dass auch bei einer verschlüsselten E-Mail der Text in der Betreffzeile weiterhin angezeigt wird.

Infos zum Versand von vertraulichen Daten mittels elektronischer Post und zur Beantragung von dafür notwendigen Zertifikaten sind erhältlich unter http://intranet.kit.edu/downloads/2014_CIO_DSB_E-Mailversand_vertraulicher_Daten.pdf.

Sie können Ihr Nutzerzertifikat online unter folgendem Link direkt beim SCC beantragen: <https://www.ca.kit.edu>

Passwort-Schutz

Ihr Rechner ist mit einer Passwortsicherung ausgerüstet. Das Passwort legen Sie selbst fest (siehe hierzu die Passwortrichtlinien des SCC unter <http://www.scc.kit.edu/dienste/4319.php>). Es wirkt wie ein Schlüssel zu Ihrem PC und zu Ihren Daten. Wer ihn hat, kann diese Daten auch unter Ihrem Namen gebrauchen, aber auch missbrauchen! Halten Sie deshalb Ihre Authentifizierungsinformationen geheim – auch gegenüber Vorgesetzten, Kollegen und Kolleginnen. Im Notfall kann ein/e Administrator/in einer berechtigten Person über ein geregeltes Verfahren Zugriff auf ihre Daten verschaffen.

Bildschirmsperre

Sperren Sie bei Verlassen Ihres Arbeitsplatzes den Bildschirm. Unter Windows können Sie dies zügig mit der Tastenkombination „Windowstaste+L“ durchführen. Richten Sie an Ihrem PC zur Sicherheit auch eine automatische Bildschirmsperre ein.

Schutz vor Schadprogrammen

Risiken durch Schadprogramme wie beispielsweise Viren, Würmer oder Trojanische Pferde können grundsätzlich nicht ausgeschlossen werden. Computer müssen über einen geeigneten Virenschutz verfügen.

Das SCC stellt Ihnen dafür einen zentralen Antivirendienst zur Verfügung (<http://www.scc.kit.edu/dienste/virenschutz.php>).

Verlust und Zerstörung von Daten

Gegen den Verlust von Daten – unbeabsichtigt oder auch unbefugt herbeigeführt – schützt die Sicherung der Daten auf externe Datenträger. Die gesicherte Aufbewahrung und kontrollierte Entsorgung von Papiausdrucken und anderen Speichermedien muss gewährleistet sein.

Das SCC stellt Ihnen dafür einen zentralen Datensicherungsdienst zur Verfügung (<http://www.scc.kit.edu/dienste/6161.php>).



Für Fragen zur IT stehen Ihnen die IT-Beauftragten an den Instituten sowie das Steinbuch Centre for Computing (SCC) Verfügung.

Nützliche Hinweise zur IT-Sicherheit am KIT finden Sie auch im Intranet des KIT unter <https://www.itsb.kit.edu> oder auch <https://www.cert.kit.edu>

Meldepflicht bei Verletzung des Schutzes personenbezogener Daten

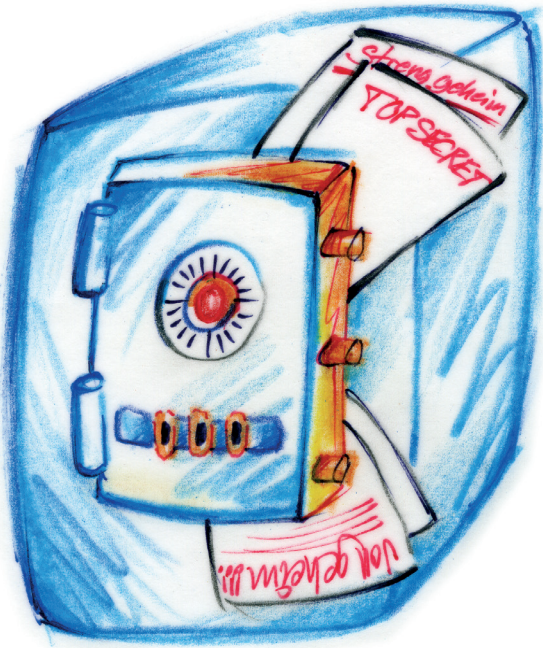
Nach der DS-GVO ist das KIT verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem dem KIT die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden (Art. 33 DS-GVO), wenn die Verletzung zu einem Risiko bezüglich der Rechte und Freiheiten natürlicher Personen führt. Des Weiteren muss das KIT die von der Verletzung betroffene Person darüber informieren, wenn die Verletzung ein hohes Risiko für deren persönliche Rechte und Freiheiten zur Folge hat (Art. 34 DS-GVO).

Sollte daher im Zusammenhang mit Ihrer Tätigkeit am KIT sich ein Vorfall ereignen, der eine Verletzung des Schutzes von personenbezogenen Daten nach sich ziehen könnte, informieren Sie umgehend Ihre OE-Leitung.

Durchführung von Schulungen in den Grundlagen des Datenschutzes

Mitarbeiterinnen und Mitarbeiter, die länger als vier Monate am KIT beschäftigt sind, haben in einem Turnus von drei Jahren eine Schulung in den Grundlagen des Datenschutzes zu absolvieren.

Das KIT bietet diese Schulung flächendeckend als E-Learning-Schulung an. Sie werden hierzu automatisch per E-Mail eingeladen und müssen selbst nichts Weiteres veranlassen.



**Wann immer Sie hinsichtlich der Verarbeitung
personenbezogener Daten Fragen haben:**

Wenden Sie sich an Ihre Datenschutzbeauftragte und/oder an die
Referenten der Stabsstelle Datenschutz (DSB).

Nützliche Hinweise zum Datenschutz finden Sie auch im
Intranet des KIT unter <http://www.dsb.kit.edu>.

Kontakt

Karlsruher Institut für Technologie (KIT)

Datenschutzbeauftragte

Ass. jur. Marina Bitmann

Telefon: +49 721 608-41057

E-Mail: marina.bitmann@kit.edu

www.dsb.kit.edu

Herausgegeben von

Karlsruher Institut für Technologie (KIT)

Präsident Prof. Dr. Jan S. Hesthaven

Kaiserstraße 12

76131 Karlsruhe

www.kit.edu

Karlsruhe © KIT 2026