Auskunftsanspruch nach Art. 15 DSGVO: Identität des Antragstellers

78. DFN-BETRIEBSTAGUNG | 28.03.2023

Ole-Christian Tech | Forschungsstelle Recht im DFN

Aufbau

- Problemaufriss
- Verschiedene Szenarien
- Lösungsansätze
- Fazit

DFN

deutsches forschungsnetz

Problemaufriss

Art. 15 DSGVO-Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

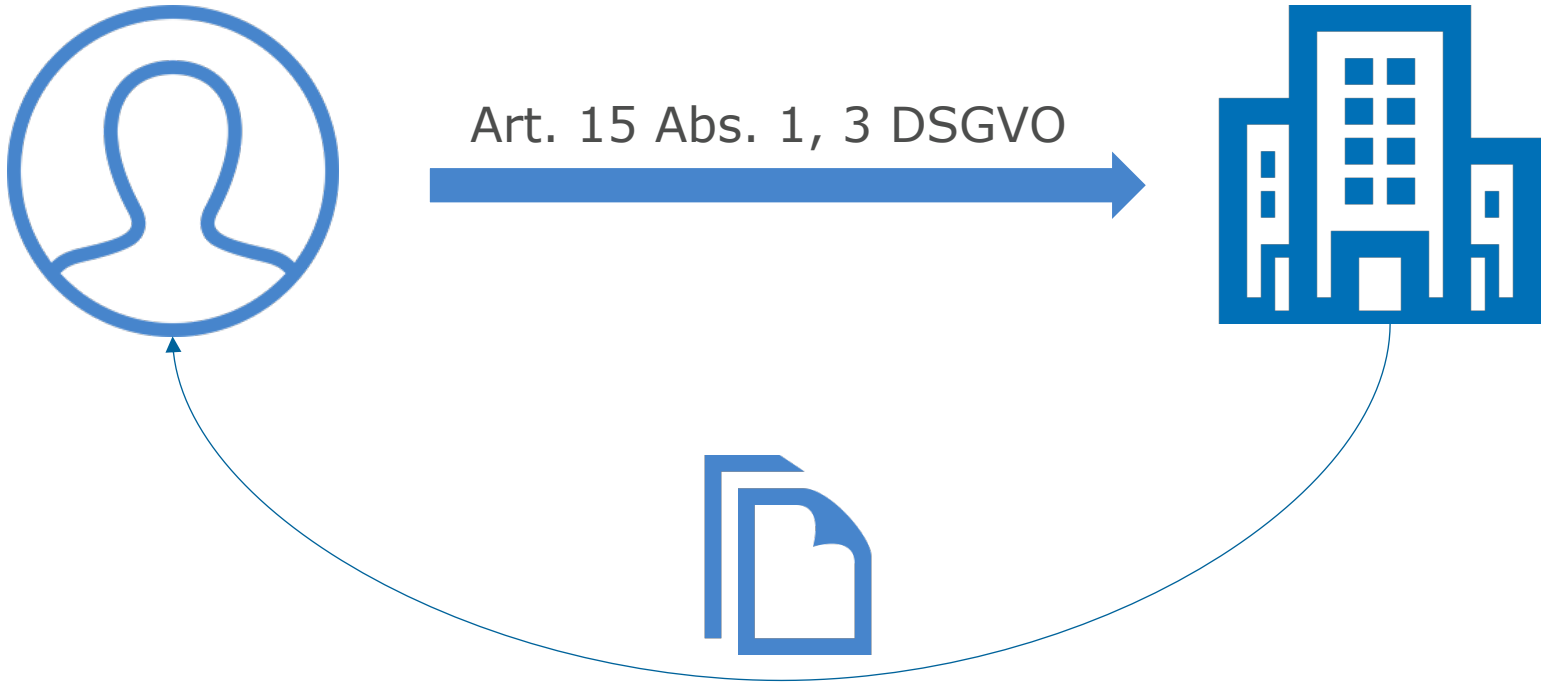
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Problemaufriss



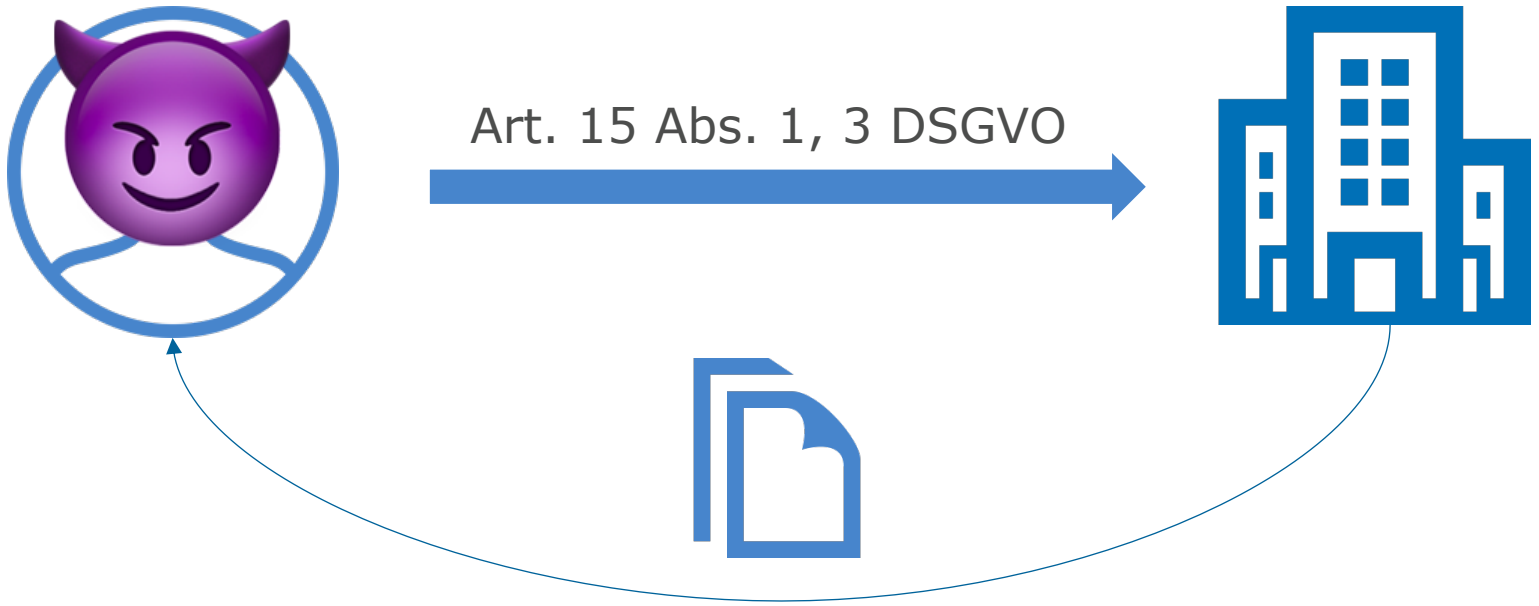
DFN

deutsches forschungsnetz

Verschiedene Szenarien

Szenario 1: „Data-Breach“

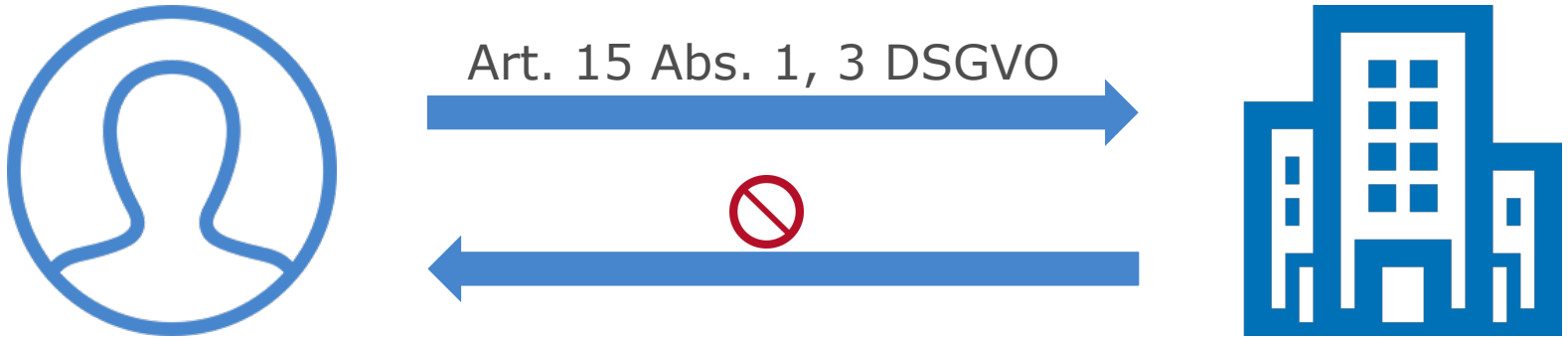
Der Verantwortliche gibt die angefragten personenbezogenen Daten an den Antragsteller heraus – der Antragsteller ist allerdings nicht der Betroffene



Szenario 2: „Verweigerung des Auskunftsbegehrens“

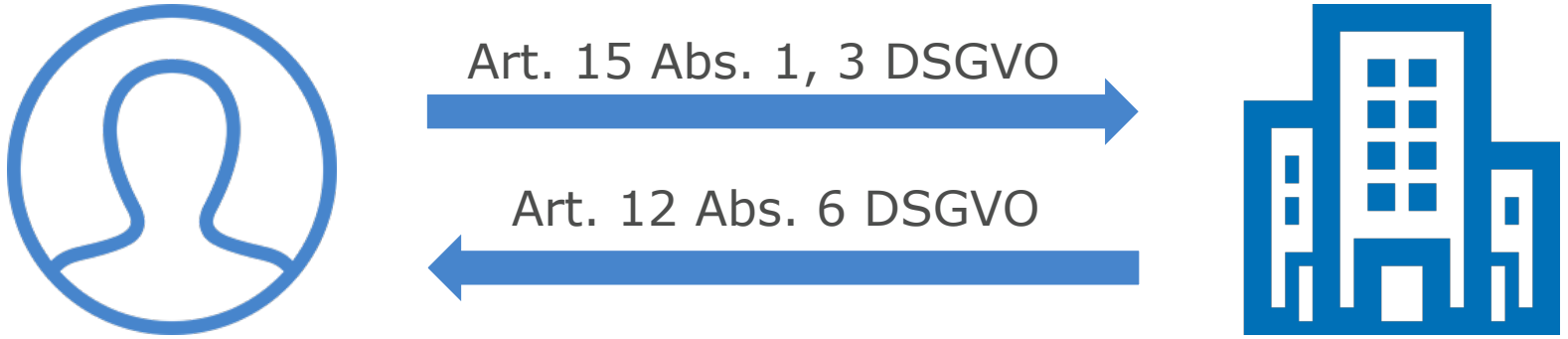
Der Betroffene stellt den Auskunftsanspruch

- Der Verantwortliche verweigert das Auskunftsbegehren jedoch, weil er Zweifel an der Identität des Anspruchsstellers hat



Szenario 3: „Exzessive Verifizierung“

Der Verantwortliche hat Zweifel an der Identität und verlangt zusätzliche Informationen zur Identifikation – hierbei fragt er jedoch unnötige oder irrelevante Informationen ab

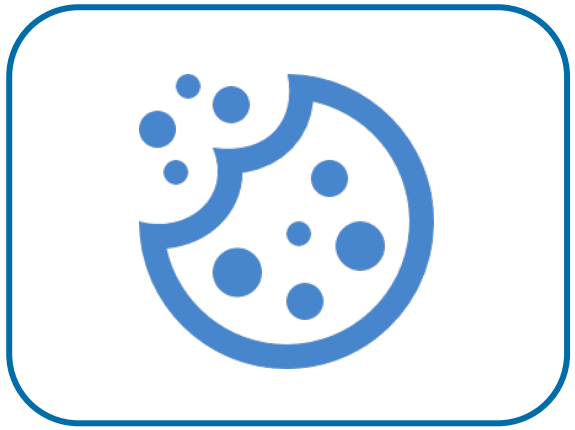


deutsches forschungsnetz

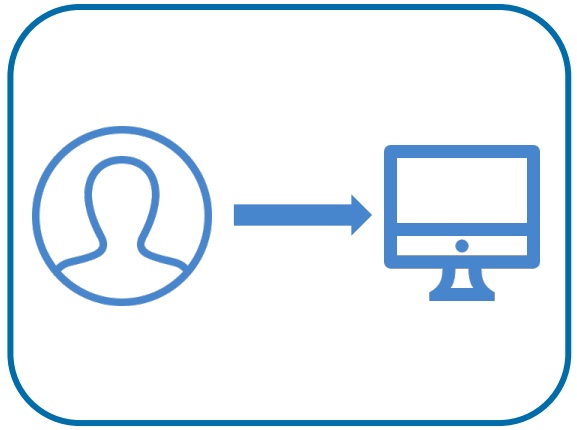
Lösungsansätze

Lösungsansätze

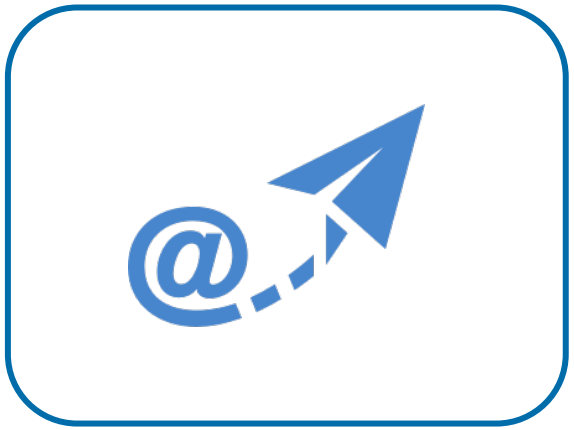
Cookies



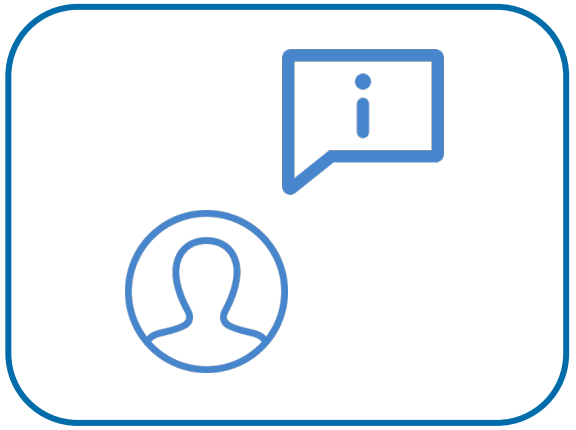
Login-Daten



E-Mail

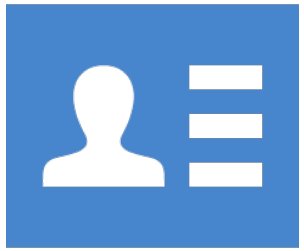


Spezifische Informationen



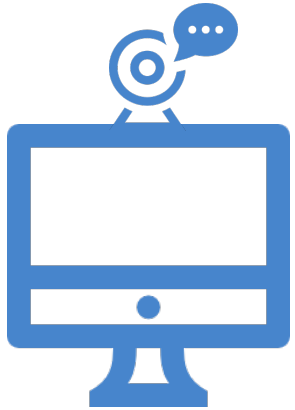
Lösungsansätze

Ausweisdokumente



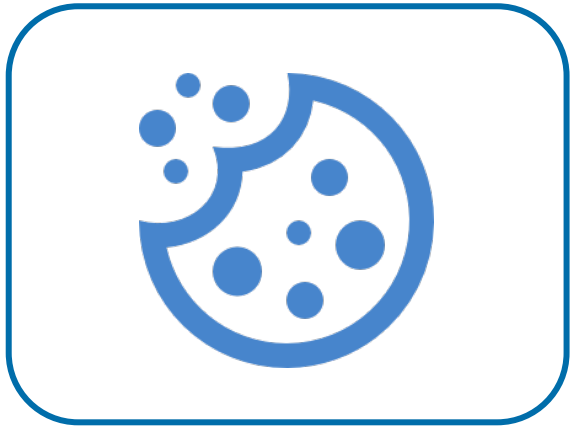
Kontrollanruf

Videoidentifikation



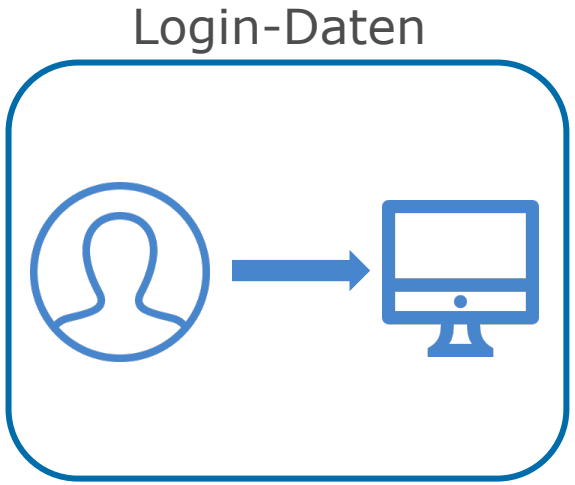
Lösungsansätze

Cookies



- Unique Identifier Cookies können zur Identifikation eines Endgeräts genutzt werden
- Vorteil: Ermöglicht Identifikation auch, wenn sonstige Kontaktdaten fehlen
- Nachteil: Einsatz von Cookies ist ggf. selbst nach § 25 Abs. 1 S. 1 TTDSG einwilligungsbedürftig

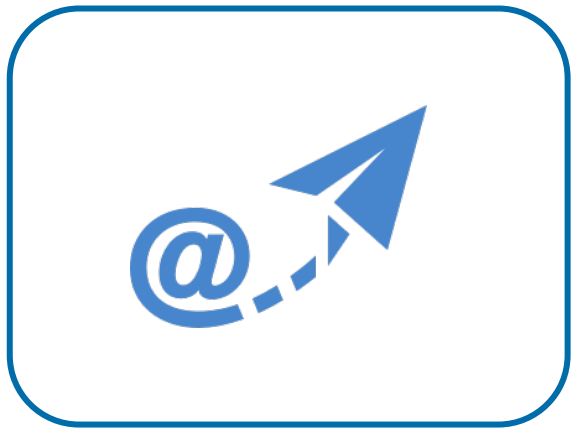
Lösungsansätze



- Login des Benutzers in Netzwerk des Verantwortlichen (z.B. Intranet, soziales Netzwerk, Selbstverwaltungsbereich etc.)
- Netzwerk ermöglicht dann Stellung der Ansprüche aus Art. 15 DSGVO
- Vorteile:
  - Relativ sicher
  - Datensparsam: Es müssen keine weiteren personenbezogenen Daten verarbeitet werden —> wenig Aufwand
  - Verordnunggeber hat diese Möglichkeit explizit in ErwG 63 S. 4 vorgesehen
- Nachteile: Nur möglich bei bereits vorliegendem Benutzersystem

Lösungsansätze

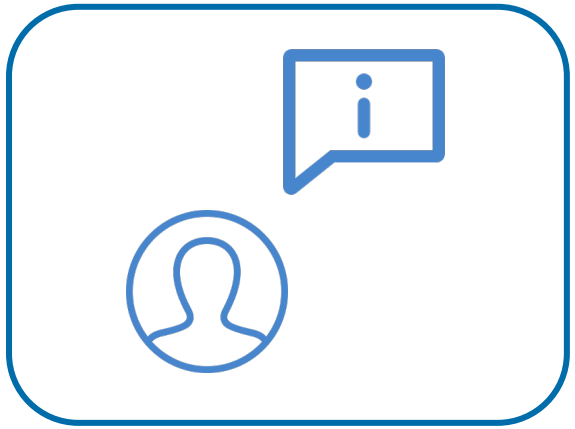
E-Mail



- E-Mail Bestätigung weist nach, dass Anspruchssteller Zugriff auf hinterlegte Mailadresse hat
- Vorteil: Relativ einfach und niedrigschwellig
- Nachteil: Nur möglich bei hinterlegter E-Mail

Lösungsansätze

Spezifische Informationen



- Abfrage betroffenenspezifischer Informationen ermöglicht Identifikation
- Sicherheitsniveau ist abhängig von abgefragten Informationen
- Vorteile:
  - Hohes Sicherheitsniveau möglich
  - Unabhängig von Logins oder Mails
- Nachteile:
  - Informationen können durch Datenlecks bekannt geworden sein
  - Gefahr sog. Daisy Chains

Lösungsansätze

Ausweisdokumente

- Überprüfung von Ausweisdokumenten zur Identifikation behördlich anerkannt (BfDI)
- Vorteile: Einfache technische Umsetzbarkeit über Scan und Zusendung per Mail
- Nachteile:
  - Erkennungszeichen wie Wassermarken gehen teilweise verloren
  - Sehr datenintensiv: Nicht erforderliche Daten sollten vorher geschwärzt werden
  - Hohes Missbrauchspotential von Ausweisdokumenten

Lösungsansätze

Kontrollanruf

- Anruf ermöglicht Identifikation
- Vorteile: Recht hohes Sicherheitsniveau
- Nachteile:
  - Gefahr der doppelten Nutzung einer Telefonnummer (Bei Festnetzanschluss)
  - Muss von hinterlegter Telefonnummer erfolgen
  - Gefahr des Telefonnummer-Spoofings

Lösungsansätze

Videoidentifikation

- Videoanruf vereint die Vorteile von Ausweisidentifikation und Kontrollanrufen
- Vorteile:
  - Sehr hohes Sicherheitsniveau
  - Ausweiskontrolle, die zahlreiche Probleme (schlechte Sichtbarkeit von Wasserzeichen etc.) umgeht
  - Zugleich Kontrollanruf ohne Risiko bei gemeinsam genutzten Telefonanschlüssen
- Nachteile: Technisch und personell aufwendig

Fazit

- Hochschulen trifft als Verantwortliche die Pflicht zur Auskunft und Kopieherausgabe nach Art. 15 Abs. 1 und Abs. 3 DSGVO
- Bei Unsicherheiten über die Identität erlaubt Art. 12 Abs. 6 DSGVO die Anfrage zusätzlicher Informationen
- Kann eine Identifikation dennoch nicht erfolgen, ist der Verantwortliche nach Art. 11 Abs. 2 S. 2 DSGVO nicht verpflichtet, Auskunft zu erteilen
- “Viel hilft viel”- nicht hilfreich
- Ignorieren oder herauszögern von Auskunftsansprüchen auch nicht

Fazit

- DSGVO ist von verschiedenen Grundsätzen geprägt, die miteinander in Einklang gebracht werden müssen
- Art. 5 Abs. 1 lit. c) DSGVO etwa verlangt die Datenminimierung und Art. 5 Abs. 1 lit. d) DSGVO die Speicherbegrenzung. Art. 5 Abs. 1 lit. f) DSGVO verlangt **geeignete** TOM, um angemessene Sicherheit vor unbefugter oder unrechtmäßiger Verarbeitung (also auch: Offenlegung) zu schaffen
- Es gibt keinen “One fits all” Ansatz, sondern ein Verhältnismäßigkeitsgebot
- Um im Betriebsablauf Sicherheit zu haben sollten Leitfaden hierzu existieren und regelmäßig überprüft werden

Haben Sie noch Fragen?

- **Kontakt**

Forschungsstelle Recht im DFN

Institut für Informations-, Telekommunikations- und Medienrecht
Zivilrechtliche Abteilung | Prof. Dr. Thomas Hoeren
Leonardo-Campus 9, 48149 Münster

E-Mail: recht@dfn.de
Telefon: 0251 83 38616