LLR
LEGERLOTZ LASCHET
RECHTSANWÄLTE
KÖLN | BRÜSSEL | HELSINKI

GRUNDZÜGE DER DATENSCHUTZ-GRUNDVERORDNUNG – DS-GVO

NEOPOST BUSINESS AFTERNOON

RA FAITR FAArbR Prof. Klaus Gennen
Telefon: +49 221 55400-170
E-Mail: klaus.gennen@llr.de

LLR Legerlotz Laschet und Partner Rechtsanwälte Partnerschaft mbB
Mevissenstraße 15
50668 Köln

Inhaltsübersicht

Grundlagen

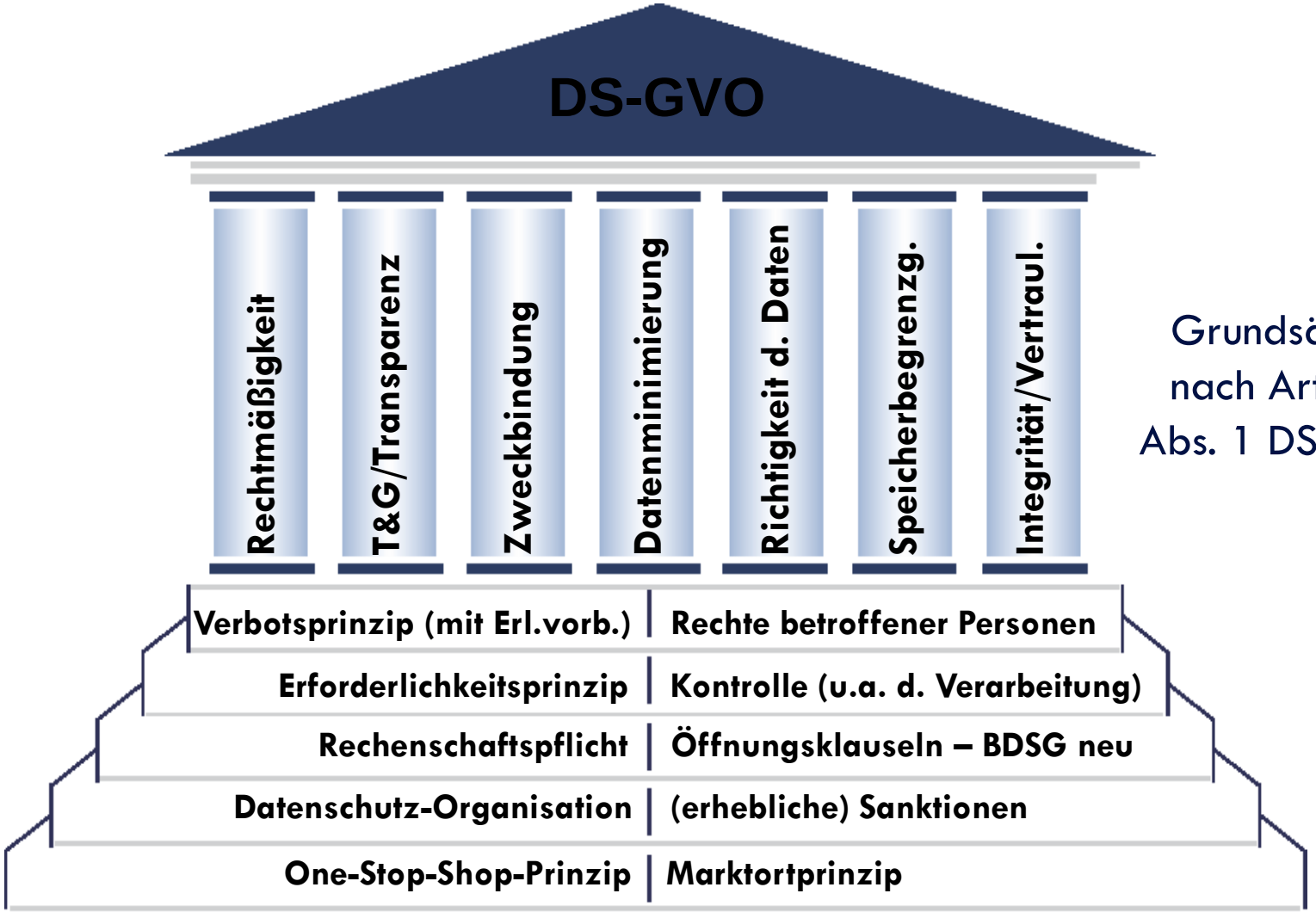
- „***Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG***“ (Datenschutz-Grundverordnung bzw. DS-GVO)
- ersetzt ab **25.5.2018** die EU-DatenschutzRL, die u.a. über das BDSG in deutsches Recht umgesetzt wurde
- VO gilt **unmittelbar**, RL wird in staatliches Recht umgesetzt
- **Öffnungsklauseln**? - BDSG wird in weiten Teilen ersetzt – DSAnpUG-NW mit neuem BDSG verabschiedet
- Herausforderung u.a. viele unbestimmte Rechtsbegriffe, neue Institutionen, keine komplette bereits bestehende Aufsichtsverwaltung
- zusätzlich: Entwurf **ePrivacy-VO** (Datenschutz für elektr. Kommunikation) in der Diskussion, lex specialis

Zielsetzung der DS-GVO

Erwägungsgrund (EG) Nr. 11

- **unionsweiter** wirksamer **Schutz** von personenbezogenen Daten [pbD]
- Stärkung und Präzisierung der **Rechte der betroffenen Person** [bP]
- **Verschärfung der Auflagen** für diejenigen, die pbD Daten verarbeiten und darüber entscheiden
- **gleiche Befugnisse der Mitgliedstaaten** bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz pbD
- **gleiche Sanktionen** im Falle ihrer Verletzung

Grundsäulen/Prinzipien der DS-GVO



Grundsätze nach Art. 5 Abs. 1 DSGVO

Rechenschaftspflicht/Beweislast

- BDSG alt: i.d.R. Nachweis Verletzung durch Aufsichtsbehörde
- DS-GVO: Nachweis Einhaltung DS-GVO durch Verantwortlichen - **Beweislast beim Verantwortlichen:** ***„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).***“
- DS-GVO: Art. 82 Abs. 3 DS-GVO – Beweislast beim Schadensers.anspruch: *„Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung […] befreit, wenn er* ***nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.***“
- **Dokumentationsaufwand** dürfte erheblich **steigen**
- **Prozesse etablieren, dokumentieren und deren Einhaltung kontrollieren und sicherstellen – „Datenschutz-Compliance“ ist erforderlich**

Bedrohungen

- Bedrohung durch **Aufsichtsbehörden**?
  - nicht oder nicht sofort
  - Verwarnung/Anweisung Vorrang vor Bußgeld (jdf. bei „Versehen“)
  - z.B. NW: kein Bußgeld bei Nachmeldung DSB bis 31.12.2018 (Webseite)
- Bedrohung durch **Abmahnanwälte**?
- Bedrohung durch **unzufriedene (ehemalige) Kunden oder Lieferanten**?
- Bedrohung durch **unzufriedene (ehemalige) Beschäftigte?**

Bußgeldrahmen (klein) – Art. 83

(4) Bei Verstößen […] werden […] **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:**

a) die **Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;**

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

Bußgeldrahmen (groß) – Art. 83

(5) Bei Verstößen […] werden […] **Geldbußen von bis zu 20 000 000 EUR** oder […] **bis zu 4 %** […] wie Abs. 4 …]:

a) die **Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Art. 5, 6, 7 und 9**;
b) die **Rechte der bP gemäß den Art. 12 bis 22;**
c) die **Übermittlung** pbD an einen Empfänger in einem **Drittland** oder an eine internationale Organisation gemäß den Art. 44 bis 49;
d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kap. IX erlassen wurden;
e) Nichtbefolgung einer Anweisung […] gemäß Art. 58 Abs. 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1.

(6) Bei **Nichtbefolgung einer Anweisung der Aufsichtsbehörde** gemäß Art. 58 Abs. 2 werden […] Geldbußen von bis zu 20 000 000 EUR oder […] bis zu 4 % […].

Kriterien für Bußgeldhöhe

Art. 83 Abs. 2 DS-GVO

a) **Art, Schwere und Dauer** des Verstoßes
b) **Verschuldensgrad**
c) vom V oder AV getroffenen Maßnahmen zur **Minderung** des den betroffenen Personen entstandenen **Schadens**
d) Grad der Verantwortung des V oder des AV unter Berücksichtigung der von ihnen **gemäß Art. 25 und 32 getroffenen TOM**
e) etwaige einschlägige **frühere Verstöße** des V oder des AV
f) Umfang der **Zusammenarbeit** mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern
g) **Kategorien** betroffener pbD
h) **Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde,** insbes. ob und ggf. in welchem Umfang der V oder der AV den Verstoß mitgeteilt hat;
i) Einhaltung der nach **Art. 58 Abs. 2** früher […] angeordneten Maßnahmen, […];
j) Einhaltung von genehmigten Verhaltensregeln nach Art. 40 oder genehmigten Zertifizierungs-verfahren nach Art. 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall […].

Bsp. Art. 30 Verzeichnis Verarbeitungstgkt.

Pflicht für Verantwortlichen [VA] (Art. 30 Abs. 1) und Auftragsverarbeiter [AV] (Art. 30 Abs. 2)

- Verzeichnis der Verarbeitungstätigkeiten
- keine Herausgabepflicht an Jedermann
- Unterschiedliche Inhalte für VA und AV
- gegenüber Aufsichtsbehörde **auf Anforderung zur Verfügung zu stellen**
- Aufzeichnungen schriftlich/elektronisch zu führen

Ausnahmen für Unternehmen < 250 Mitarbeiter, sofern Verarbeitung nicht **Risiko für Rechte/Freiheiten der betroffenen Person** birgt, nur **gelegentlich** erfolgt oder **nicht besondere Datenkategorien** (Art. 9 DS-GVO) oder Straftaten (Art. 10 DS-GVO) einschließt.

Sanktionsrahmen bis 10 Mio. Euro / 2 % des Vorjahresumsatzes

Bsp. Art. 32 TOM / DSK

Art. 32 Abs. 1 – „Sicherheit der Verarbeitung“

- Zielsetzung: Gewährleistung eines dem Risiko angemessenen Schutzniveaus

Umsetzung

- durch geeignete technische und organisatorische Maßnahmen (TOM),
- die getroffen werden unter Berücksichtigung
  - des **Stands der Technik,**
  - der **Implementierungskosten,**
  - der **Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung,** sowie
  - der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere des Risikos** für die persönlichen Rechte und Freiheiten

Bsp. Art. 32 TOM / DSK

Art. 32 Abs. 1 – „Sicherheit der Verarbeitung“

… diese TOM schließen u.a. Folgendes ein:

- **Pseudonymisierung** und **Verschlüsselung** von pbD
- Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzustellen**
- Fähigkeit, die **Verfügbarkeit** der pbD und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der TOM zur Gewährleistung der Sicherheit der Verarbeitung

Sanktionsrahmen bis 10. Mio. Euro / 2 % des Vorjahresumsatzes
Beachten: Gilt auch bei **Auftragsverarbeitung**

Bsp. Art. 12-23 Rechte der betroff. Person

Überblick

- **transparente Information und Kommunikation** (Art. 12),
- **Informationspflichten** bei Datenerhebung (Art. 13, Art. 14),
- **Auskunftsrecht** (Art. 15),
- Recht auf **Berichtigung** (Art. 16),
- Recht auf **Löschung** (Art. 17) [*Recht auf Vergessenwerden*],
- Recht auf **Einschränkung** der Verarbeitung (Art. 18),
- Recht auf **Datenübertragbarkeit** (Art. 20),
- **Widerspruchsrechte** (Art. 21),
- **Profiling** und automatisierte Einzelentscheidungen (Art. 22),
- die Möglichkeit der **Beschränkung** … durch Rechtsvorschriften der Union oder der Mitgliedstaaten (Art. 23).

Bsp. Art. 37 betriebl. Datenschutzbeauftr.

- **Erfordernis der Bestellung eines DSB?**
  - **Behörde/öffentl. Stelle**
  - Kerntätigkeit besteht in Durchführung von Verarbeitungsvorgängen, die aufgrund Art, Umfang und/oder Zweck eine **umfangreiche regelmäßige und systematische Überwachung von bP erforderlich** machen
  - Kerntätigkeit besteht in umfangreicher Verarbeitung besonderer Kategorien von pbD nach **Art. 9** (oder Daten nach **Art. 10**)
- Anzahl der Mitarbeiter/mit der Verarbeitung befasster Mitarbeiter irrelevant!
- aber – **Öffnungsklausel** in Art. 37 Abs. 4 DS-GVO – § 38 BDSG (neu)
- Weitere Fälle:
  - mind. 10 Personen ständig mit automatisierter Verarbtg. von pbD befasst
  - Verarbtg., die einer Datenschutz-Folgenabschätzung unterliegen
  - geschäftsmäßige Verarbtg. zu Zwecken der (anonymisierten) Übermittlung oder Markt- und Meinungsforschung

Bsp. Art. 28 Auftragsverarbeitung

Grundsatz der Privilegierung bleibt bestehen

- Auftragsverarbeiter **kein Dritter,** Art. 4 Abs. 10 DS-GVO

Verantwortlicher bleibt im Grds. für Verarbeitung verantwortlich

- Pflichtinhalte Vertrag bei der Beauftragung
- Angemessenheit der Schutzmaßnahmen
- Nachweis ausreichender Schutzmaßnahmen
- Auftragsverarbeiter wird mit in die Haftung genommen
- Einbindung von Subunternehmern formalisierter geregelt

⇨ **NEU**: geänderte inhaltliche Anforderungen an die Vereinbarung

⇨ **NEU**: gemeinsame Haftg. (Art. 28) Verantwortlicher und Auftragsverarbeiter

⇨ **Überprüfungsbedarf ADV!**

Sanktionsrahmen bis **10 Mio. Euro / 2 % des Vorjahresumsatzes**

⇨**auch gegen AV möglich**

⇨**NEU:** Risiko für Auftragsverarbeiter ⇔ Haftung mit Verantwortlichem

Bsp. Art. 28 Auftragsverarbeitung

Inhaltliche Anforderungen an Vertrag, Art. 28 Abs. 3 DS-GVO

*„Die Verarbeitung durch einen AV erfolgt auf der Grundlage eines Vertrags … der … den AV in Bezug auf den V bindet und in dem **Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der pbD, die Kategorien betroffener Personen und die Pflichten und Rechte des V** festgelegt sind. Dieser Vertrag … sieht **insbes.** vor, dass der AV*

a) *die pbD nur auf **dokumentierte Weisung** des V - auch in Bezug auf die Übermittlung von pbD an ein **Drittland** oder eine internationale Organisation - verarbeitet, […];*

b) *gewährleistet, dass sich die zur Verarbeitung der pbD befugten **Personen zur Vertraulichkeit verpflichtet** haben oder einer **angemessenen gesetzlichen Verschwiegenheitspflicht** unterliegen;*

c) *alle gemäß **Artikel 32 erforderlichen Maßnahmen** ergreift;*

d) *die in den Absätzen 2 und 4 genannten **Bedingungen für die Inanspruchnahme der Dienste eines weiteren AV einhält**;*

e) *angesichts der Art der Verarbeitung den V nach Möglichkeit mit geeigneten TOM dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;*

f) *unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen **den V bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt**;*

f) *nach Abschluss der Erbringung der Verarbeitungsleistungen alle pbD **nach Wahl des V entweder löscht oder zurückgibt**, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der pbD besteht;*

g) *dem V **alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt** und **Überprüfungen - einschließlich Inspektionen –,** die vom V oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, **ermöglicht und dazu beiträgt**.*

*Mit Blick auf Unterabsatz 1 Buchstabe h informiert der AV den V unverzüglich, falls er der **Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.“***

Schadensersatzansprüche

Ersatzansprüche nach Art. 79, 82 DS-GVO

- immaterielle Schäden eingeschlossen, s.a. EG 146 Satz 3 DS-GVO
- Beweislast aufseiten Verantwortlichem/Auftragsverarbeiter, aber Möglichkeit der Enthaftung bei **Nachweis nicht vorhandener Verantwortlichkeit** (Art. 82 Abs. 3 DS-GVO)
  *„Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn **er nachweist**, dass er **in keinerlei Hinsicht** für den Umstand, durch den der Schaden eingetreten ist, **verantwortlich** ist.“*
- Notwendigkeit zur vertraglichen Haftungsfreistellung im Innenverhältnis? Art. 82 Abs. 5 DS-GVO

Welche konkreten Schritte?

- *Ressourcen allokieren, im Unternehmen Verständnis wecken*
- **Aufnahme der Ist-Prozesse** im räumlichen/sachlichen Anwendungsbereich der DS-GVO
- **Erarbeitung einer Risikoanalyse** für jede/n der vorhandenen Geschäftsprozesse und –situationen, in denen pbD zur Verarbeitung anstehen
- Ableitung eines DS-GVO-konformen **Soll-Zustandes** aufgrund der Risikoanalyse
- **Schließen einer evtl. Lücke zwischen Ist- und Soll-Zustand,** bis Konformität mit der DS-GVO erreicht ist
- **Etablieren und Ausrollen einer gut dokumentierten Datenschutz-organisation,** die selbstständig fortgeführt werden kann und die insbesondere in der Lage ist, der Rechenschaftspflicht zu genügen

Beratung: Notwendige Unterlagen?

- **Organigramm** jeder konzernzugehörigen Gesellschaft, aus dem erkennbar ist, welche Abtlg. für die Verarbtg. welcher Art von pbD verantwortlich sind
- alle **Verfahrensverzeichnisse**
- **Zertifizierungen** mit datenschutzrechtlichem Einschlag (ISO 27001)
- Aufstellungen der ergriffenen **TOM** einschl. **Löschkonzepte**
- Ergebnisse vorgenommener **Vorabkontrollen**
- Ergebnisse vorgenommener **Risikoanalysen**
- **Datenschutzhandbuch**
- **Dienstanweisungen** mit datenschutzrechtl. Einschlag, einschl. Dienstanweisungen zu Organisationsfragen
- **Rechte- und Rollenkonzepte** für alle IT-Systeme
- **Formularwesen** im Bereich Datenschutz oder mit Berührung zum Datenschutz
- **BVen** mit datenschutzrechtl. Einschlag (insbes. § 87 Abs. 1 Nr. 6 BetrVG)
- Was ist sonst vorhanden?

Betroffene Bereiche? Mindestens …

- **Zweck**festlegung/-änderung
- **Verarbeitungsverzeichnis**
- **Datensicherheit**
- Einsatz **datensparsamer** Systeme/DP by design
- **Datenschutzfreundliche** Voreinstellungen in Systemen/DP by default
- Recht auf **Datenübertragbarkeit**
- Reaktionsmechanismen betreffend **Daten(schutz)verletzungen**
- **Informationspflichten** bei Datenerhebung
- **Auskunftsrecht** der betroffenen Person
- **Löschkonzepte**
- „Recht auf **Vergessenwerden**“
- Recht auf Einschränkung der Verarbeitung
- **Widerspruchsrecht**
- Recht auf **Berichtigung**
- **Datenschutzfolgeabschätzung**
- **Auftragsverarbeitung** (ggf. gemeinsam Verantwortliche)
- Übermittlung von Daten in **Drittstaaten**
- Einrichtung eines effektiven und risikoangemessenen **Beschwerdemanagements**
- **Vertragsmanagement**
- **Einwilligungsmanagement**
- Bestehende **Betriebsvereinbarungen**?
- Notwendigkeit von **Schulungen**
- **Einbindung von Rechtsabteilung, Compliance, IT-Security, DSB**

Ihr Referent

Prof. Klaus Gennen

- Rechtsanwalt seit 1993
- Fachanwalt für IT-Recht
- Fachanwalt für Arbeitsrecht
- Betrieblicher Datenschutzbeauftragter (GDDcert.)
- verantwortlich für das Dezernat IT/Datenschutz
- Geschäftsführer der LLR DSC GmbH (www.llrdsc.de)
- ordentliche Professur (Teilzeit) an der TH Köln, Kölner Forschungsstelle für Medienrecht (IT-Recht, E-Commerce, IT-Vergaberecht)

LLR
LEGERLOTZ LASCHET
RECHTSANWÄLTE
KÖLN | BRÜSSEL | HELSINKI

DANKE …
FÜR IHRE AUFMERKSAMKEIT

RA FAITR FAArbR Prof. Klaus Gennen
Telefon: +49 221 55400-170
E-Mail: klaus.gennen@llr.de

LLR Legerlotz Laschet und Partner Rechtsanwälte Partnerschaft mbB
Mevissenstraße 15
50668 Köln