



BVMed - Datenschutz im Gesundheitswesen

Nachweispflichten und Umgang mit Datenpannen

1. Oktober 2025 - RAin Maria Heil

Agenda



Rechtsgrundlagen Accountability



Umfang und Reichweite Nachweispflichten



Wann liegt eine Datenpanne vor?



Melde-/Benachrichtigungspflichten bei Datenpannen



Handlungsempfehlungen

RECHTSGRUNDLAGEN ACCOUNTABILITY

Grundsatz der Nachweis- und Rechenschaftspflicht

Gesamtverantwortung des Verantwortlichen für seine Verarbeitung personenbezogener Daten



Art. 5 Abs. 2 DSGVO: Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“)



Art. 24 Abs. 1 DSGVO: Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

Nachweis Einhaltung Grundpflichten und Einhaltung angemessener TOMs (risikobasiert)

Festlegung interner Strategien und Maßnahmen

Pflichterfüllung nur möglich durch umfassende Dokumentation der internen Datenschutzprozesse

Transparentes und effizientes Datenschutzmanagement erforderlich



UMFANG NACHWEISPFlichten

Umfang der Pflicht für Unternehmen

- DSGVO selbst keine Aussage zum Umfang und Granularität der Nachweispflicht
- Form und Umfang liegen in Verantwortung des Datenverantwortlichen
- Zweck Accountability: Einfachere Prüfmöglichkeit der Aufsichtsbehörden hinsichtlich der Rechtmäßigkeit der Datenverarbeitung
- Umfassende Nachweispflichten?
 - Kaum umsetzbar, insbesondere nicht von KMU
 - Risikobasierter Ansatz: Umfang TOM je nach Risiko für Betroffene
 - Nachweis als Teil der unternehmerischen Compliance
- Zeitliche Grenze?
 - Nicht ausdrücklich vorgesehen
 - Verjährung Ordnungswidrigkeiten?

Umsetzung Nachweis- und Rechenschaftspflicht (Beispiele)

- Einhaltung genehmigter Verhaltensregeln oder Zertifizierungsverfahren (Nachweisunterstützung)
- Führung Verarbeitungsverzeichnis
- Datenschutzmanagementsystem
- Datenschutz-Folgenabschätzung (Beschreibung und Bewertung geplanter Verarbeitungsvorgänge)
- Benennung eines Datenschutzbeauftragten
- Informations- und Auskunftspflichten
- Datensicherheitskonzept
- Zugriffs- und Berechtigungskonzept
- Löschkonzept
- Dokumentation und Meldung von Datenpannen

- Regelmäßige Kontrollpflicht, ob Nachweis erbracht werden kann
- Verantwortlicher muss Maßnahmen überprüfen und notfalls aktualisieren, anpassen oder austauschen

- Art. 58 Abs. 1 lit. a DSGVO
 - Kontrolle durch die Datenschutz-Aufsichtsbehörde
 - Behörde kann sich notwendige Informationen zur Erbringung des Nachweises der Verarbeitung anhand der DSGVO vorlegen lassen
 - Darlegungs- und Beweislast in Streitfällen Datenverantwortlicher

- Bußgeldrahmen Art. 83 DSGVO
- Art. 24 Abs. 1 DSGVO iVm mit jeweiliger Pflichtennorm
- Verstoß gegen Dokumentation datenschutzrechtlicher Verpflichtung
- Ohne Nachweis der Einhaltung der Grundsätze keine Befreiung von Haftung möglich

UMGANG MIT DATENPANNEN

Datenpannen – Beispiele aus der Gesundheitsbranche

Datenpanne

Patientendaten von Fresenius Medical Care in Serbien gehackt

Der Dialyseanbieter Fresenius Medical Care (FMC) bestätigt, dass es in Folge eines Hackerangriffs zur illegalen Veröffentlichung von Patientendaten gekommen ist. Betroffen sind einige Dialysezentren in Serbien.

Sechsstelliges Bußgeld

Uniklinik wird für Datenpanne bestraft

Der rheinland-pfälzische Landesdatenschutzbeauftragte statuiert ein Exempel: Die Uniklinik Mainz muss ein sechsstelliges Bußgeld für Verstöße gegen die Datenschutzgrundverordnung zahlen.

Von Matthias Mollenhahn

Datenpanne bei Blutspendedienst bestätigt

31. Mai 2021, 15:21 Uhr | Lesezeit: 2 Min.

PFLEGER VERLIERT RUCKSACK MIT PATIENTEN-DATEN. BETROFFENE SIND EN

Daten-Skandal im Krankenhaus!

HIV-Infektion, Krebs, Drogenkonsum: Beim Online-Check zur Blutspende wurden private Informationen an Facebook übermittelt. Damit hat der Blutspendedienst des Bayerischen Roten Kreuzes gegen Datenschutzgesetze verstoßen.

DATENPANNE

Merck Österreich verliert sensible Daten von 2000 Patienten

Sensible Daten waren einsehbar Sicherheitsleck beim Roten Kreuz in Brandenburg

Das Deutsche Rote Kreuz in Brandenburg hat nach Bekanntwerden einer Sicherheitslücke beim Datenschutz Strafanzeige gegen Unbekannt erstattet.

Bußgelder wg. Datenpannen

Irland	• Speicherung von Passwörtern von ca. 36 Mi. Facebook- und Instagram-Nutzenden im Klartext in internen Datenbanken, keine angemessenen Sicherheitsmaßnahmen und nicht ausreichende Dokumentation der Sicherheitslücke, verspätete Meldung an Behörde (2 Monate nach Kenntnisnahme) (EUR 91 Mio.)
Italien	• Ungeschützter Versand einer Krankenakte wg. nicht ausreichender Schulung eines Mitarbeiters (EUR 24.000)
Italien	• Verspätete und unzureichende Information Betroffener über einen Sicherheitsvorfall durch italienisches Gesundheitsministerium (EUR 100.000)
Deutschland	• Offenlegung von Gesundheitsdaten durch Verpflichtung zur Krankmeldung per E-Mail-Verteiler (EUR 75.000)
Italien	• Mangelhafte Entsorgung von Gesundheitsdokumenten aus nicht mehr genutztem Sanatorium (EUR 50.000)
Schweden	• Gesprächsaufzeichnungen eines medizinischen Beratungsdienstes wegen falscher Konfiguration ungeschützt auf Webserver gespeichert (EUR 1.566.125)
Frankreich	• Unbefugte Offenlegung von Gesundheitsdaten von fast 500.000 Personen seitens Anbieter von medizinischer Software wegen mangelhaftem Zugangsschutz auf Webserver (EUR 1.500.000)
Portugal	• Unerlaubter Zugriff für Techniker sowie andere Unberechtigte auf Patientendaten in IT-System eines Krankenhauses durch mangelhaftes Berechtigungsmanagement (EUR 400.000)

- Begriff „Datenpanne“ umgangssprachlich
- Art. 33 Abs. 1 DSGVO **„Verletzung des Schutzes personenbezogener Daten“**
- Legaldefinition in Art. 4 Nr. 12 DSGVO: *„Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurde“*

Wann liegt eine Datenpanne vor?

Vertraulichkeitsverletzung

- Unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten.

Offenlegung
personenbezogener
Daten

Integritätsverletzung

- Unbefugte oder unbeabsichtigte Änderung personenbezogener Daten.

Verletzung der
Datensicherheit!

Verfügbarkeitsverletzung

- Unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten.

Kein Vorsatz
erforderlich,
„Versehen“ genügt!

Wann liegt eine Datenpanne vor?

Elementarschaden
(Brand) mit Datenverlust
aufgrund unzureichender
Implementierung eines
Back-up-Konzepts

Fehler bei der
Übermittlung von Daten
an die falschen
Adressaten.

Verschlüsselung durch
einen Ransomware-
Angriff

Hackerangriffe mit
Datendiebstahl oder -
offenlegung

Versehentliche
Offenlegung durch
falsche Konfiguration

Phishing-Angriffe

Diebstahl/Verlust von
Hardware (Laptop,
Dokumente etc.)

Unzureichende
Zugangskontrollen

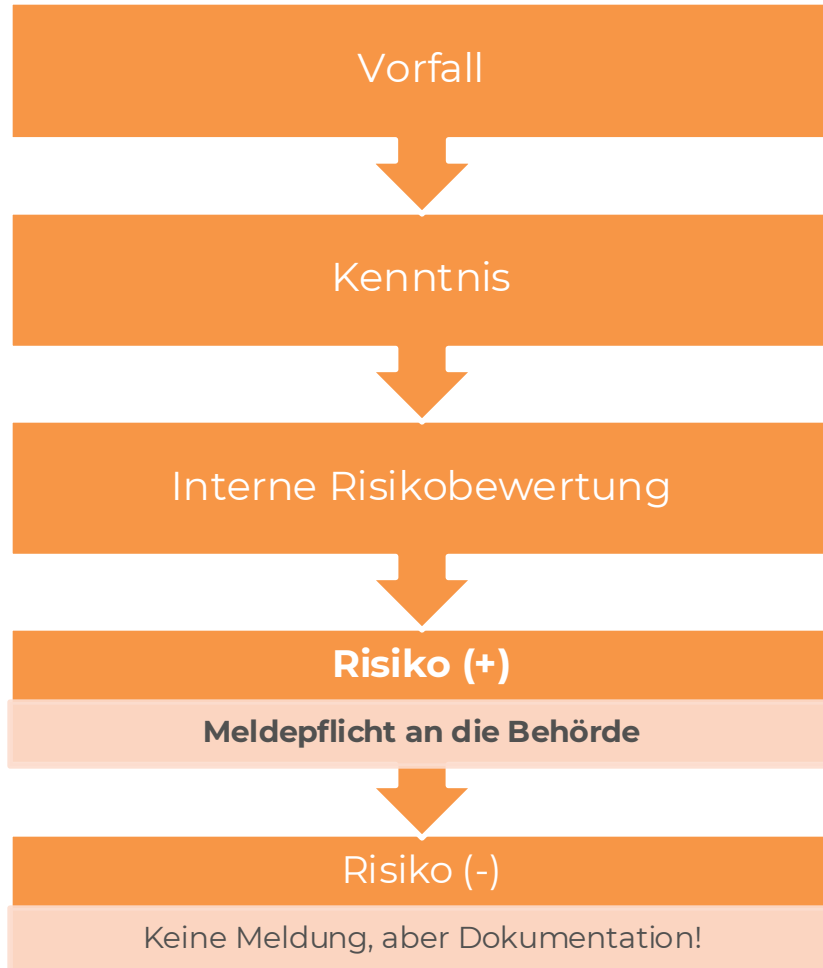


- Feststellung des Sachverhalts
 - Sind personenbezogene Daten betroffen?
 - Ist eine Verletzung der Datensicherheit aufgetreten?
 - Welche Ad-Hoc-Gegenmaßnahmen kommen in Betracht (z. B. Vernichtung der Unterlagen bei Fehlversand)

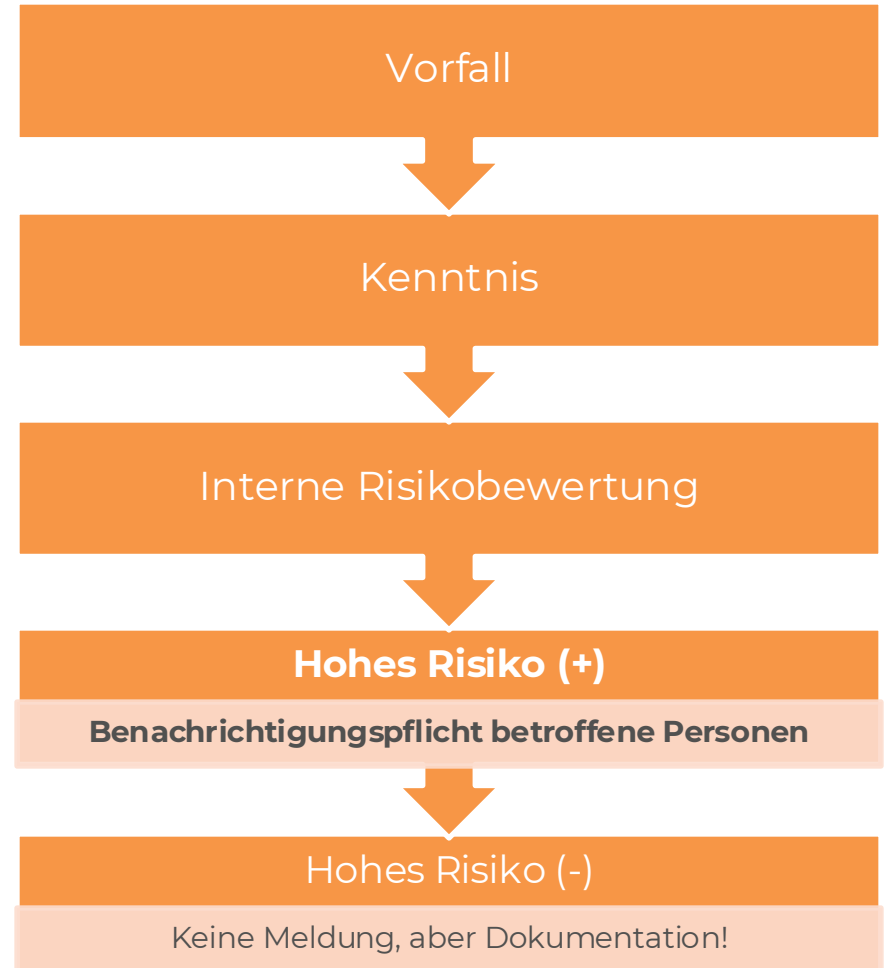
MELDE- UND BENACHRICHTIGUNGSPFLICHTE N

Melde-/ Benachrichtigungspflichten

Behörde



Betroffene Personen



- Art. 33 Abs. 1 DSGVO: Grds. **Meldepflicht** bei Datenschutzverletzung
- Meldung an die zuständige Aufsichtsbehörde (Art. 55 DSGVO)
- Verantwortlich: Datenschutzverantwortlicher
 - Prüfung Sachverhalt, Risiko und einzuleitende Maßnahmen
- Frist: „**Unverzüglich** und möglichst binnen **72 Stunden**“ nach Bekanntwerden
- Fristauslösendes Ereignis: **Bekanntwerden** der tatsächlichen Umstände (Sicherheitsverletzung sowie Verletzung des Schutzes personenbezogener Daten)



Zumindest kurzer Untersuchungszeitraum, allerdings keine rechtlich umfassende fundierte Prüfung möglich

- Ausnahmsweise keine Meldepflicht, wenn **voraussichtlich** kein **Risiko** für die Rechte und Freiheiten natürlicher Personen
- Begriff Risiko: Erhöhte Eintrittswahrscheinlichkeit eines drohenden Schadensereignisses (Erw. 75, 95 DSGVO)
- Physischer, materieller oder immaterieller Schaden
- Risikobeurteilung durch Prognoseentscheidung

- Art 34 DSGVO: Benachrichtigung der betroffenen Personen erforderlich, wenn
 - Voraussichtlich **hohes Risiko** für die persönlichen Rechte und Freiheiten
 - „Betroffene“: Natürliche Personen, deren Daten Gegenstand der Datenschutzverletzung sind (z.B. Patienten, Mitarbeiter)
- Frist: „unverzüglich“, d.h. so schnell wie möglich („ohne schuldhaftes Zögern“)!
- Ausnahmen: Art. 34 Abs. 3 DSGVO (z. B. unverhältnismäßiger Aufwand, dann aber öffentliche Bekanntmachung o.ä.)

Mögliche Risiken für die Betroffenen?

Erwägungs-
grund 85

Verlust der Kontrolle über die eigenen Daten

Diskriminierung, Rufschädigung, Imageverlust

Identitätsdiebstahl oder -betrug

Finanzielle Verluste

Unbefugte Aufhebung der Pseudonymisierung

Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen (z.B. Gesundheitsdaten)

Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

Art. 29-
Daten-
schutz-
gruppe

Art der Datenschutzverletzung

Sensibilität und Umfang der beeinträchtigten Daten
(z.B. sensible Daten)

Identifizierbarkeit betroffener Personen

Schwere der (potentiellen) Folgen für die betroffenen
Personen

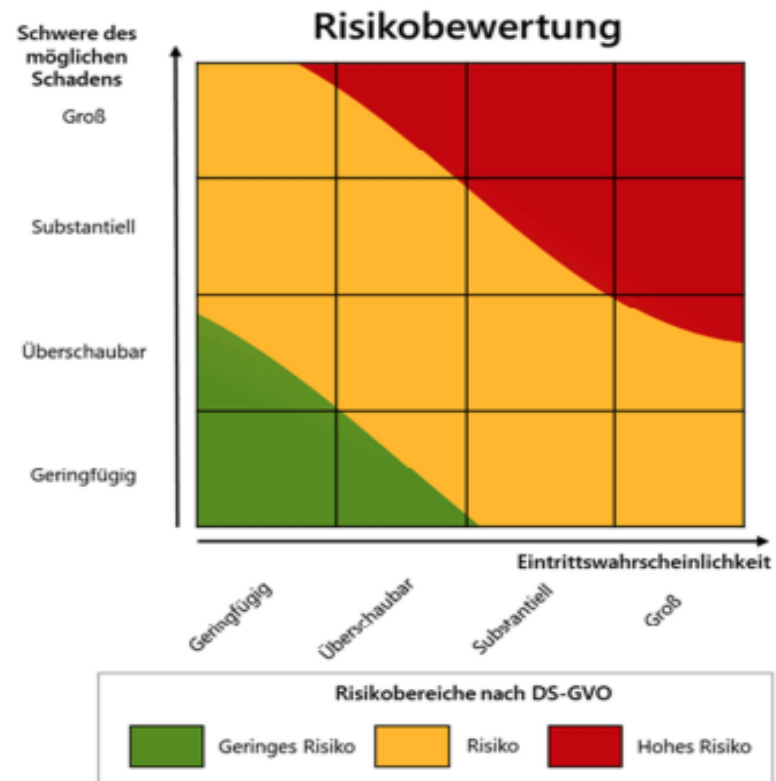
Besondere Eigenschaften der betroffenen Person

Besondere Eigenschaften des Verantwortlichen

Zahl der betroffenen Personen

Risikobewertung

- Identifizierung von Risiken
- Abschätzung
Eintrittswahrscheinlichkeit
- Schwere möglicher
Schäden
- Zuordnung zu Risikostufen



Bei Unklarheiten: Vorabkonsultation der Behörde!
Ggf. auch vorsorgliche Meldung möglich

- Art. 33 Abs. 3 DSGVO
 - Art der Verletzung
 - Name und Kontaktdaten des Datenschutzbeauftragten
 - Beschreibung der wahrscheinlichen Folgen der Verletzung
 - Entsprechende Gegenmaßnahmen
 - Alle dt. Datenschutzbehörden halten elektronische Meldeportale bereit, in dringlichen Fällen auch telefonische Meldung möglich
- Art. 34 DSGVO (Benachrichtigung betroffene Personen): Beschreibung der Datenschutzverletzung in klarer und einfacher Sprache

Erwägungsgrund 87:

„Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.“

- Interner Prozess zum Erkennen und Melden von Verstößen unabdingbar!
- Accountability!
- Art. 33 Abs. 5 DSGVO: Umfassende Dokumentationspflicht

- Art. 83 Abs. 4 DSGVO: Verhängung von **Bußgeldern** durch die Aufsichtsbehörden (bis zu 10 Mio. EUR oder bis zu 2 % des Vorjahresumsatzes eines Unternehmens)
- Art. 58 DSGVO: Weitere mögliche Maßnahmen der Aufsichtsbehörden (Auskunft / Untersuchung, Anordnung Verwarnung)
- Art. 82 DSGVO: (Immaterieller) **Schadenersatzanspruch** („Schmerzensgeld“)

HANDLUNGSEMPFEHLUNGEN

- Implementierung interner Prüf- und Meldeprozesse
- Vorherige Festlegung der genauen Vorgehensweise bei Verdacht eines Vorfalls
- Sofortige Einleitung der erforderlichen Schritte

Prüfung und Diagnose – Maßnahmen zur schnellen Kenntniserlangung

- Interne Richtlinie / Arbeitsanweisung für den internen Umgang mit Datenpannen
- Festlegung einer internen Meldestelle (z.B. Datenschutzkoordinator, Datenschutzbeauftragter)
- Internes Wissensmanagement
 - Intranet und Handout sowie Prozessbeschreibungen, die allen Mitarbeitern bekannt sind
 - Sensibilisierung der eigenen Mitarbeiter (Schulungen)
- Ggf. Einführung Ticketsystem mit Zeitstempel und Zuständigkeiten zur genauen Dokumentation
- Interne Meldeformulare / Fragebögen entsprechend den Anforderungen aus Art. 33 Abs. 3 DSGVO zur schnellen Aufklärung des Sachverhalts

- Interner Prozess zur sofortigen Einleitung der Prüfung des Vorgangs (Urlaubsvertretungen regeln!)
- Klare Zuständigkeitszuweisung: z.B. Datenschutzteam, rechtzeitige Einbindung des Datenschutzbeauftragten, ggf. interne/externe IT-Dienstleister, externe Berater
- Erfassung des Sachverhalts und Klärung bzw. Erforschung der Ursachen und Auswirkungen
- Bewertung des Vorfalls: Leitlinien, Kriterienkataloge oder Bewertungsmatrix zur Ermöglichung einer schnellen und möglichst einfachen Bewertung und Risikoanalyse

Einleitung kurzfristiger Maßnahmen

- Schadensabwehr: Sofortige Gegenmaßnahmen zur schnellen Eindämmung der Verletzung und möglicher Risiken (z. B. Schließen von Sicherheitslücken, Abschalten befallener Systeme, Sperrung von Zugängen)
- Ggf. Aktivierung Notfallkonzept
- Entscheidung über die Meldung des Vorfalls und Benachrichtigung der betroffenen Personen: Einbindung der Geschäftsführung!
- Laufende Fristenkontrolle: Gewährleistung der Einhaltung der Melde-/ Benachrichtigungsfrist
- Präventivmaßnahmen zur Vermeidung vergleichbarer Verstöße in der Zukunft

- Feststellung der zuständigen Aufsichtsbehörde
- Meldung an Aufsichtsbehörde über elektronisches Meldeportal
- Ggf. als abgestufte Meldung, wenn Vorgang noch nicht abschließend bewertet
- Spätere Erkenntnisse können durch nachträgliche Meldung nachgereicht/aktualisiert werden (Art. 33 Abs. 4 DSGVO)
- Mögliche freiwillige Benachrichtigung an Betroffene

- Dokumentationspflicht des gesamten Vorfalls für Zeitraum von drei Jahren
- Gilt auch für nicht meldepflichtige Vorfälle!
- Dokumentation zu Nachweiszwecken (Accountability): Nachweis z.B. bei Nachfrage seitens Behörde
- Regelmäßige Audits zur Aufdeckung und Behebung von Schwächen der internen Prozesse

- Fehlerdiagnose
- Verbesserung TOMs
- Schulung von Mitarbeitern (was ist passiert und warum)
- Anpassung Personalstruktur
- Regelmäßige Überprüfung

Nachweispflichten und Präventivmaßnahmen für Datenpannen ernst nehmen

Robuste interne Prozesse reduzieren Risiken für Unternehmen und erleichtern Umgang mit Datenpannen

Datenstrategie im Unternehmen wichtig, Umsetzung und Know-How auf allen Mitarbeitererebenen erforderlich

Im Fall der Fälle: An interne Prozesse halten, ggf. auch vorsorglich Behörde einschalten und Betroffene informieren



VIELEN DANK!

Maria Heil, M.C.L.
Shadowplatz 12
D-40212 Düsseldorf

T +49 211 9099 3665
F +49 211 9099 3699
maria.heil@novacos-law.com
www.novacos-law.com

© 2024 NOVACOS Rechtsanwälte
Heil Hübner Natz Oeben Stallberg Partnerschaft mbB
Sitz Düsseldorf I AG Essen PR 3581

