

Was ein Administrator über Datenschutz wissen muss

Berlin, 14.05.2014

Rechtsanwalt Thomas Feil
Fachanwalt für IT-Recht und Arbeitsrecht
Datenschutzbeauftragter TÜV

**"Jeder Mensch soll grundsätzlich selbst über die
Preisgabe und Verwendung seiner persönlichen
Daten bestimmen."**

Volkszählungsurteil, 1983

§ 1 BDSG

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

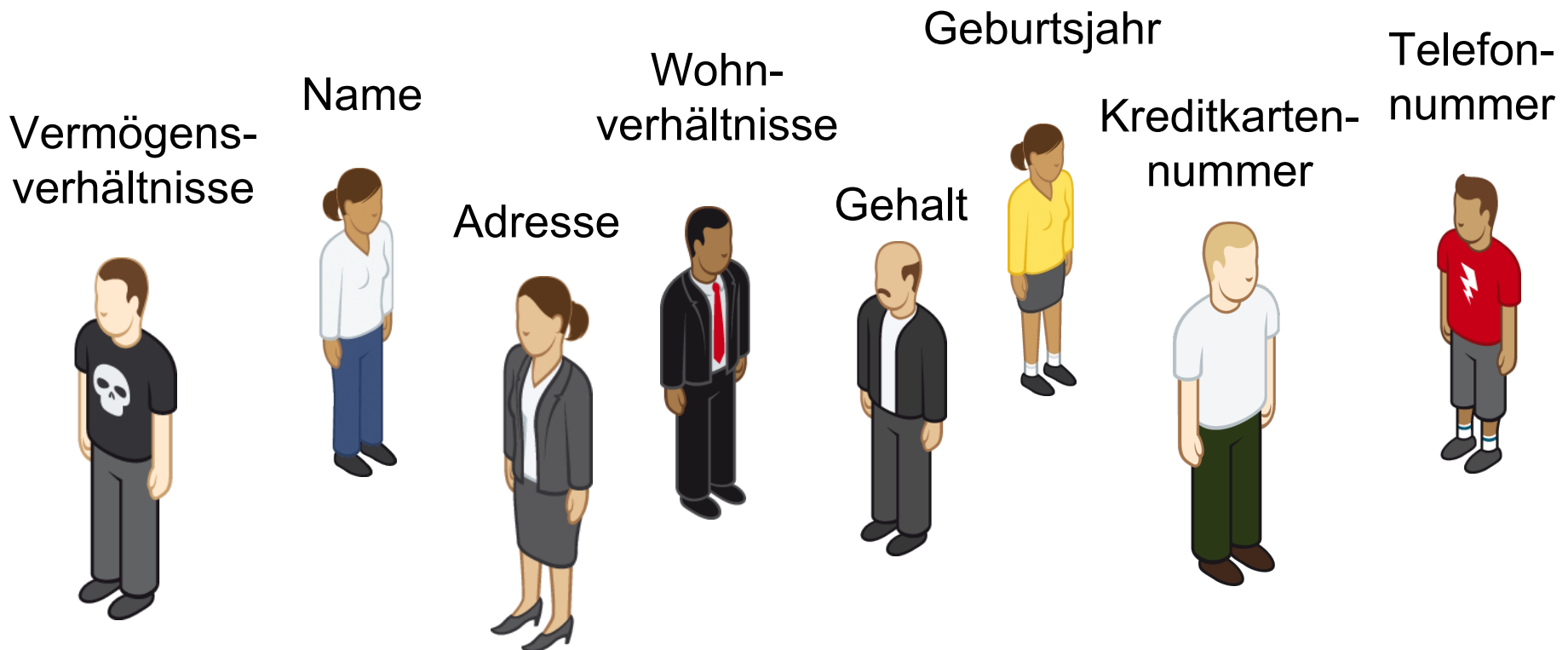
Um was geht es im Datenschutz?

§ 3 BDSG

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.

Beispiele:



Bestimmt ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Name

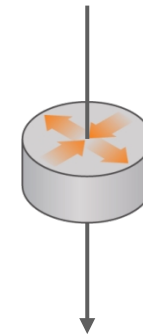


Bestimmt ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Bestimmbar wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.



IP-Adresse



Abgleich mit
Providerdaten



Weitaus strengere Regeln gibt es für den Umgang mit sogenannten besonderen Arten personenbezogener Daten, da diese besonders schützenswert sind.

Politische
Meinung



Gewerkschafts-
zugehörigkeit



Rassische
und ethnische
Herkunft



Religiöse oder
philosophische
Überzeugung



Gesundheit



Sexual-
leben



Die Daten von juristischen Personen,
Vereinen, Verbänden etc. sind im BDSG
nicht geschützt.

Grundlinien des Datenschutzes



Das BDSG schützt die personenbezogenen Daten von Menschen.



Grundannahme im Datenschutz: Es ist alles verboten!

Das BDSG verbietet grundsätzlich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, erlaubt diese aber unter bestimmten Voraussetzungen (Verbot mit Erlaubnisvorbehalt).

Datenerhebung ist somit zulässig, wenn sie ...



durch das BDSG selbst ...

Beispiel: öffentlich zugängliche Daten



oder durch eine andere Rechtsvorschrift ...

Beispiel: Steuern, Abgaben



oder durch die Einwilligung des Betroffenen ...

Beispiel: Einverständniserklärung zur Datennutzung

... erlaubt wird.

Versteckte Einwilligungen zulässig?

§ 4a BDSG

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Anruf nach der Reparatur

Ein Rechtsanwalt ließ die Windschutzscheibe seines Autos austauschen, weil sie gerissen war. Als er den Reparaturauftrag erteilte, bat ihn das Autoglasunternehmen darum, für den "Fall der Fälle" doch bitte seine Handynummer zu hinterlassen. Das tat er bereitwillig, denn es war ja denkbar, dass es irgendwelche Rückfragen geben könnte. Solche Nachfragen waren dann jedoch nicht erforderlich. Der Reparaturauftrag wurde erledigt und bezahlt.

Der Anwalt glaubte deshalb, die Sache mit der Telefonnummer sei erledigt. Umso überraschter war er, als er kurz danach einen Anruf von einem Marktforschungsunternehmen erhielt. Es hatte von dem Autoglasunternehmen den Auftrag erhalten, Kunden nach ihrer Zufriedenheit mit der Abwicklung von Reparaturen zu befragen.

OLG Köln: Zulässig?

Zweckbindung

Das Gebot der Zweckbindung soll sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben worden sind.

Erforderlichkeit

Keine zumutbare Alternative

Datensparsamkeit

Die Grundidee ist, dass bei der Datenverarbeitung nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind.

Datenschutzbeauftragter

- ▶ Bestellt werden darf nur, wer die erforderliche Sachkenntnis und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit anderen dienstlichen Aufgaben ausgesetzt ist.
- ▶ Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin.
- ▶ Unterrichtung über geplante Verfahren zur Verarbeitung personenbezogener Daten

Wer ist verantwortlich?

Behördenleitung

Sie trägt die Verantwortung für den Datenschutz nach innen und außen.

Führungskraft

Sie sorgt für die Umsetzung und Kontrolle der Einhaltung gesetzlicher und interner betrieblicher Regelungen.

Mitarbeiter

Sie sind u. a. für den Schutz pbD Daten vor unbefugtem Zugriff und unzulässiger Weitergabe zuständig.

Personalrat

Als Vertretung der Mitarbeiter wirkt er im Rahmen der Mitbestimmung auf einen mitarbeiterorientierten Datenschutz hin.



Datenschutzbeauftragter

Er wirkt auf die Einhaltung des Datenschutzes hin.

Alle sind verantwortlich!

Kundenname / Logo	<u>Verfahrensdokumentation</u> Teil 1 zu veröffentlichende Angaben gem. § 4g Abs. 2 S. 1 i.V.m. § 4e S. 1 BDSG	Version 1.0
-------------------	---	-------------

Name des Verfahrens: / Verfahrensnummer

1. Name oder Firma der verantwortlichen Stelle:

2. Vertretung

2.1 Namen der Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter

2.2 Namen der mit der Leitung der Datenverarbeitung beauftragten Personen:

2.3 Ansprechpartner:

3. Anschrift der verantwortlichen Stelle:

Straße:

Postleitzahl:

Ort:

Telefon:

Telefax:

eMail:

4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung:

Mit Angabe der Rechtsgrundlage.

5. Betroffenen Personengruppen und diesbezügliche Daten:

5.1 Beschreibung der betroffenen Personengruppen:

5.2 Beschreibung der diesbezügliche Daten oder Datenkategorien:

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:

7. Regelfristen für die Löschung der Daten:

8. Datenübermittlung in Drittstaaten:

- ☐ Datenübermittlung findet wie folgt statt
- ☐ Datenübermittlung ist in folgendem Umfang geplant
- ☐ Datenübermittlung findet nicht statt und ist auch nicht geplant.

9. Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind

9.1 Art der eingesetzten Datenverarbeitungsanlagen

9.2 Art der eingesetzten Software

9.3 Maßnahmen zum Schutz der Daten oder Datenkategorien (§ 9 BDSG)
Erläuterungen:

- | | |
|--|----------------------|
| ☐ Zutrittskontrolle | <input type="text"/> |
| ☐ Zugangskontrolle | <input type="text"/> |
| ☐ Zugriffskontrolle | <input type="text"/> |
| ☐ Weitergabekontrolle | <input type="text"/> |
| ☐ Eingabekontrolle | <input type="text"/> |
| ☐ Auftragskontrolle | <input type="text"/> |
| ☐ Verfügbarkeitskontrolle | <input type="text"/> |
| ☐ Trennungskontrolle | <input type="text"/> |

10. Angabe der zugriffsberechtigten Personen / Personengruppen

11. Verfahrenshistorie

Verfahren gemeldet durch

Verfahren eingeführt am >Datum eingeben<

Verfahren erfasst am >Datum eingeben<

Verfahren kontrolliert am (fortlaufend dokumentieren) >Datum eingeben<

Verfahren kontrolliert durch

Vorabkontrolle erforderlich ☐ ja / ☐ nein

Vorabkontrolle durchgeführt am >Datum eingeben<

12. Bemerkungen / Maßnahmen

Erforderliche Maßnahmen:

Bemerkungen:

Anmerkungen des DSB:

Dauerbrenner:

Privatnutzung Mail/Internet im Arbeitsverhältnis

3 Stunden pro Tag Naturbilder anschauen



Die zentrale Weichenstellung

Privatnutzung geduldet oder erlaubt?

Kritisch

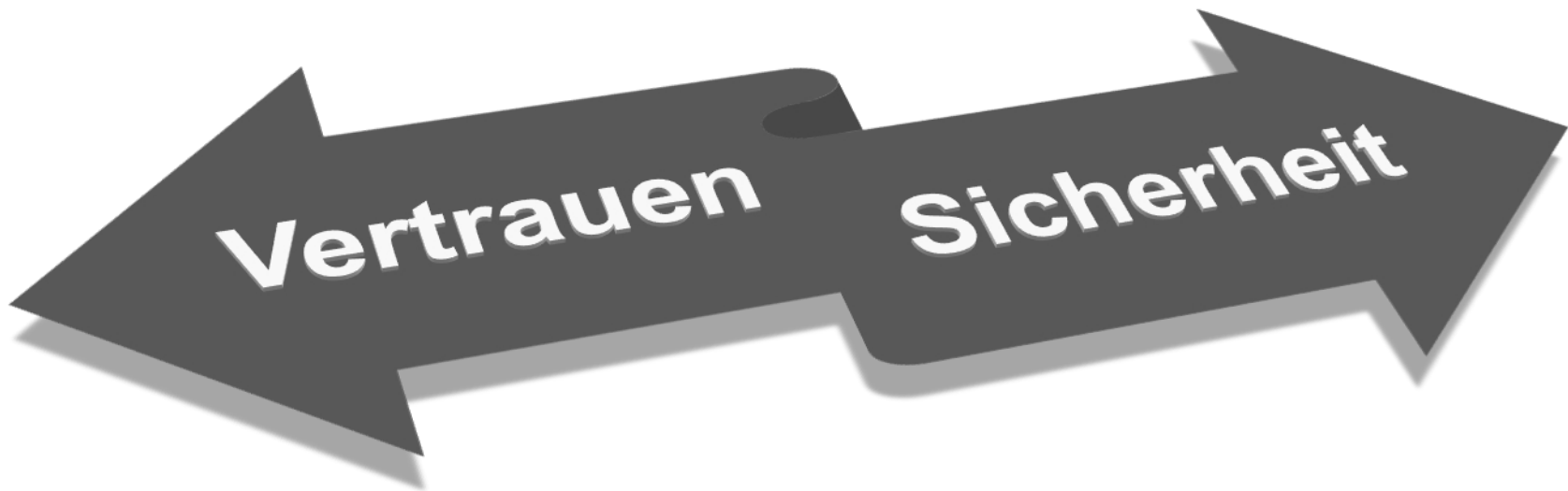
- ▶ Herausgabe von Passworten
 - aus Sicht des Administrators: notwendig (?)
 - aus Sicht des Arbeitnehmers: „gefährlich“
 - aus Sicht der Geschäftsleitung: Vertrauen und Kontrolle

- ▶ Zugriff auf PC-Arbeitsplätze bei erlaubter oder geduldeter Privatnutzung

- ▶ Individuelle Auswertungen über MitarbeiterInnen, z.B. auf Wunsch von Geschäftsleitungen oder Vorgesetzten

Cloud Computing aus datenschutzrechtlicher Sicht







**Die erste wichtige Weichenstellung
für Ihr Cloud-Projekt:**

Welche Daten gehen in die Cloud?

Welche Daten gehen in die Cloud?

- Personenbezogene Daten
- Besondere Arten von personenbezogenen Daten
- Steuerlich relevante Daten
- Produktionsdaten oder sonstige Daten

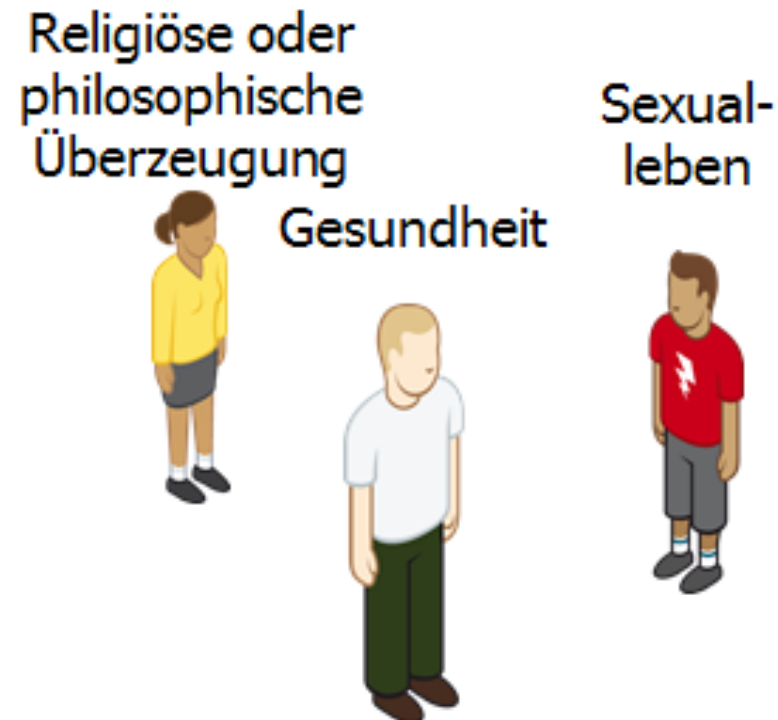
Personenbezogene Daten

- ▶ Nicht die Menge ist entscheidend
- ▶ Datenschutz
 - Werden Daten „weitergegeben“?
 - In welches Land?
 - Bleibt die Verantwortung beim Auftraggeber?
- ▶ Auftragsdatenverarbeitung und die Folgen des § 11 BDSG

Name



- ▶ Nicht die Menge ist entscheidend
- ▶ Datenschutz
 - Werden Daten „weitergegeben“?
 - In welches Land?
 - Bleibt die Verantwortung beim Auftraggeber?
- ▶ Auftragsdatenverarbeitung und die Folgen des § 11 BDSG



Steuerlich relevante Daten

- ▶ Fragen Sie Ihr Finanzamt!
- ▶ Spannend!
 - § 146 Abs. 2 AO: Bücher und die sonst erforderlichen Aufzeichnungen sind im Geltungsbereich dieses Gesetzes zu führen und aufzubewahren.
 - § 146 Abs. 2a AO: Abweichend von Absatz 2 Satz 1 kann die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs dieses Gesetzes geführt und aufbewahrt werden können.

Produktionsdaten, sonstige Daten

- ▶ Datenschutz anwendbar?
- ▶ Anforderungen an IT-Sicherheit
- ▶ Schutz von Geschäftsgeheimnissen



Datenschutzrechtliche Anforderungen an Fernwartung

Wartungsarbeiten

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Heißt u.a.:

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

Bring your own Device

Datenschutz



- ▶ Schutz der personenbezogenen Daten ist zu beachten, auch wenn private Geräte eingesetzt werden.
- ▶ Wenn Unternehmen betriebliche Kunden- oder Mitarbeiterdaten auf privaten Endgeräten eines Mitarbeiters, wird diese Mitarbeiter zum Auftragnehmer dieser Personendatenverarbeitung. Der Arbeitgeber als Auftraggeber muss mit dem Mitarbeiter schriftlich, d.h. mit eigenhändiger Unterschrift, einen detaillierten geregelten Vertrag über diese Auftragsdatenverarbeitung schließen (§ 11 BDSG).

Wenn nicht

- ▶ Wird keine Vereinbarung über die Auftragsdatenverarbeitung geschlossen, riskiert der Arbeitgeber ein Bußgeld von bis zu 50.000 Euro.
- ▶ Der Arbeitgeber muss sicherstellen, dass ein Mitarbeiter im Auftragsverhältnis alle erforderlichen Datenschutz- und Datensicherungsmaßnahmen trifft, um den unberechtigten Zugriff Dritter auf betriebliche Daten zu verhindern.
- ▶ Der Arbeitgeber darf bei personenbezogenen Datenverarbeitung keine Dienste von Internet-Provider nutzen, die diese Daten in Drittstaaten verwalten.

Haben Sie noch Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Rechtsanwalt Thomas Feil

Fachanwalt für Informationstechnologierecht und Arbeitsrecht
Datenschutzschutzbeauftragter TÜV - Geschäftsführer

Döhrbruch 62 · 30559 Hannover

Tel 0511 / 473906-0

Fax 0511 / 473906-7

feil@recht-freundlich.de