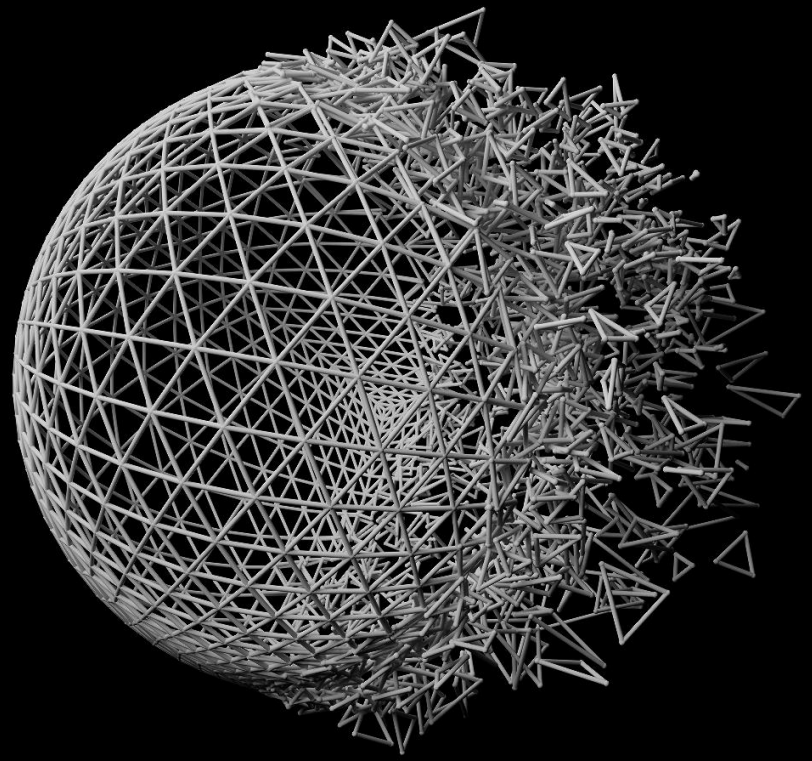
Deloitte.
Legal



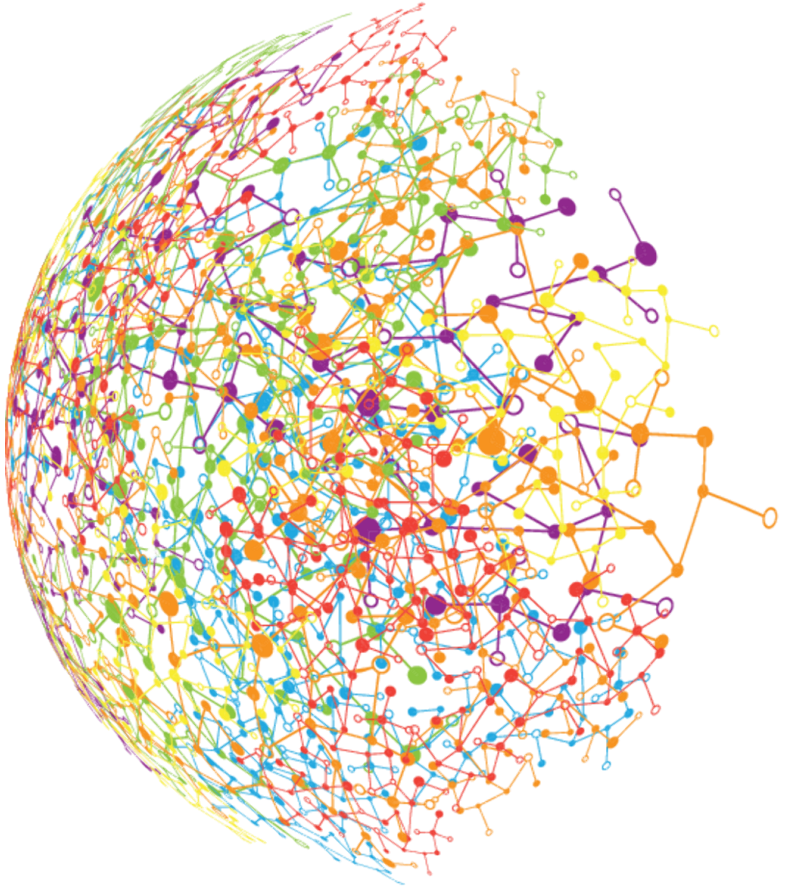
Digitalisierung der Personalabteilung

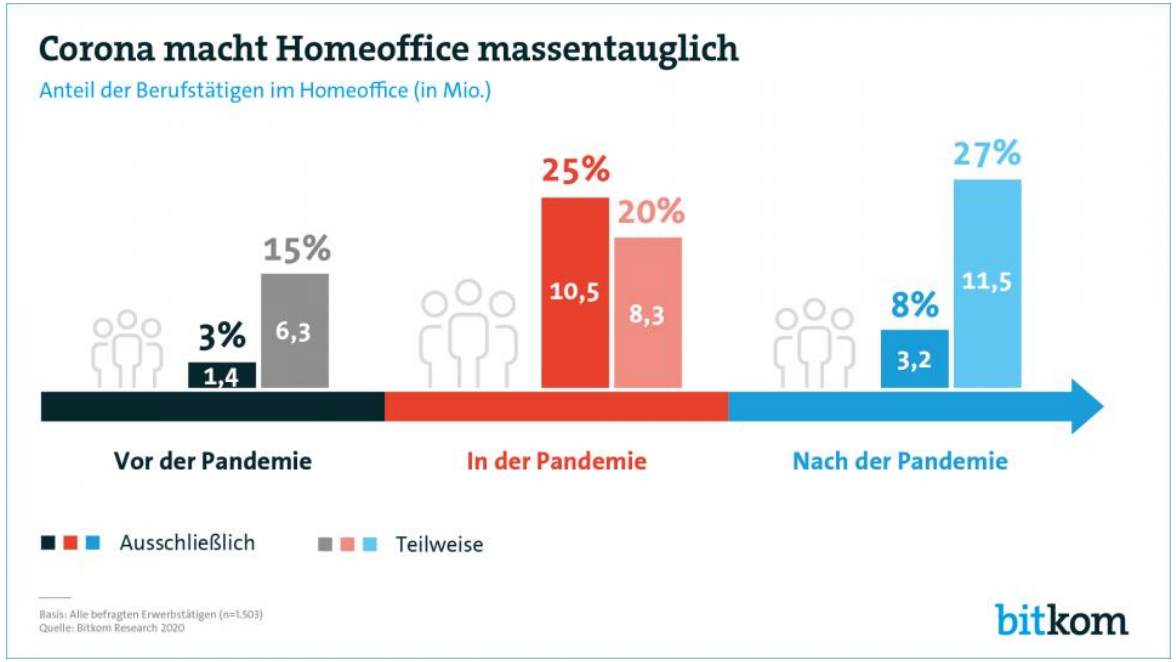
Rechtliche Aspekte des Umgangs mit Arbeitnehmerdaten

Deloitte Legal Webcast | 13. Oktober 2021

MAKING AN IMPACT THAT MATTERS since 1845

Inhaltsübersicht





Handelsblatt

MEINE NEWS | HOME POLITIK UNTERNEHMEN TECHNOLOGIE FINANZEN AUTO KARRIERE ARTS & STYLE MEINUNG VIDEO SERVICE

The Shift! Chef zu gewinnen Handelsblatt macht Schule

Handelsblatt > Karriere > Clubhouse: Wofür die Hype-App im Recruiting taugt

Suchbegriff, WKN, ISIN

TALENTSUCHE

Clubhouse: Wofür die Hype-App im Recruiting taugt und wofür nicht

Die Audioapp Clubhouse sorgt für einen Hype. Statt Stellenanzeigen zu schalten, werben hier Unternehmen für Stellen. Was Personaler und Jobsuchende davon lernen können.

LArbG Baden-Württemberg Urteil vom 14.3.2019, 17 Sa 52/18

Außerordentliche Kündigung - üble Nachrede per WhatsApp an Kollegin

Leitsätze

Verbreitet eine Arbeitnehmerin eine unzutreffende Behauptung, die geeignet ist, den Ruf eines Kollegen erheblich zu beeinträchtigen (hier: die unzutreffende Behauptung, der Kollege sei wegen Vergewaltigung verurteilt worden) per WhatsApp an eine andere Kollegin, kann dies einen Grund darstellen, der den Arbeitgeber auch zur außerordentlichen Kündigung des Arbeitsverhältnisses berechtigt.

Übersicht über den Arbeitnehmerdatenschutz

Abgrenzung von DSGVO und BDSG

Grundsatz: Datenschutzrecht aus der EU-Datenschutzgrundverordnung

Personenbezogene Daten
=
alle Informationen, die direkt oder indirekt einen Rückschluss auf eine bestimmte Person zulassen (z.B. Name, Mailadresse, Standortdaten, Aussehen)

Verantwortlicher
=
diejenige natürliche oder juristische Person, die personenbezogene Daten verarbeitet

Verarbeitung
=
jeder automatisierte und nicht-automatisierte Vorgang, bei dem personenbezogene Daten verwendet werden

Datenverarbeitung im Arbeitsverhältnis ist weiterhin im nationalen Recht geregelt (§ 26 BDSG)

Verantwortlicher
=
Arbeitgeber

Übersicht über den Arbeitnehmerdatenschutz

Anwendungsbereich von § 26 BDSG

Die vorrangig anzuwendende Datenschutzregelung im Arbeitsverhältnis in § 26 Bundesdatenschutzgesetz (BDSG) hat ihren eigenen Anwendungsbereich:

1. Persönlicher Anwendungsbereich

Grundsätzlich werden folgende im Betrieb beschäftigte Personen von der Regelung erfasst (§ 26 Abs. 8 BDSG):

- **Arbeitnehmer**
- Leiharbeitnehmer
- Auszubildende
- Freiwilligendienstleistende
- Arbeitnehmerähnliche Personen
- Heimarbeiter und gleichgestellte Personen
- Beamte, Richter, Soldaten und Zivildienstleistende
- Besondere Arbeitnehmergruppen mit Behinderung oder Rehabilitanden
- **Bewerber**
- **gekündigte Arbeitnehmer**

2. Sachlicher Anwendungsbereich

Erfasst wird entsprechend der Datenschutzgrundverordnung (DSGVO) jeder Datenverarbeitungsvorgang, wobei es insbesondere nicht darauf ankommt, ob die verarbeiteten Daten auf einem Datensystem dauerhaft gespeichert werden (§ 26 Abs. 7 BDSG).

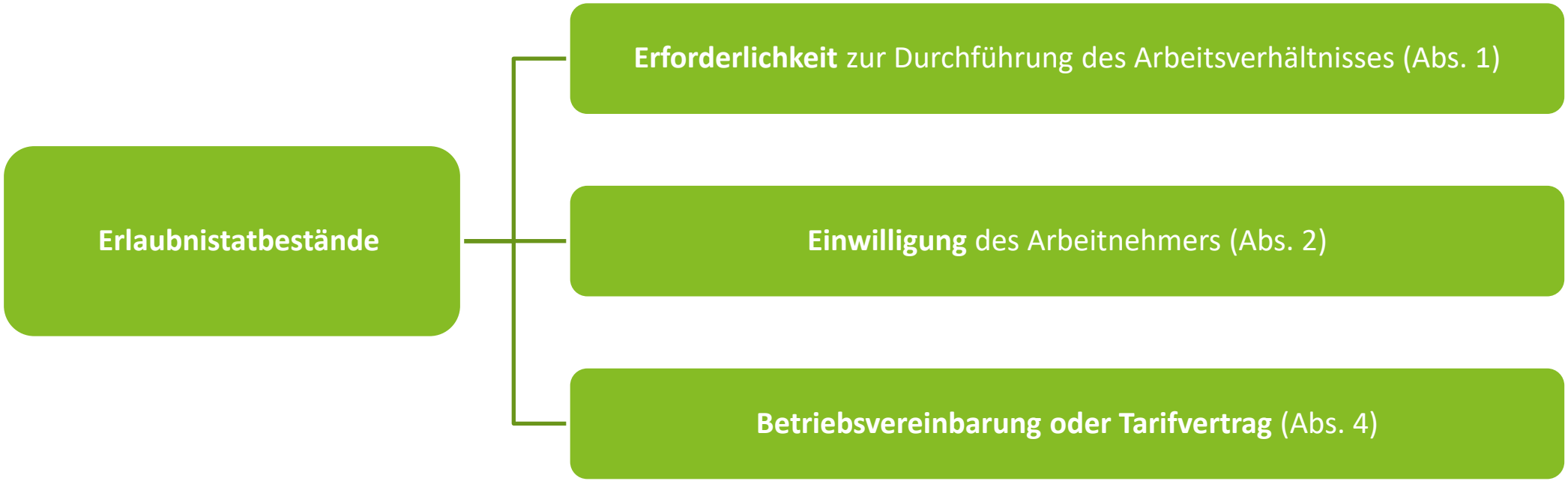
3. Räumlicher Anwendungsbereich

Das BDSG gilt nur im Inland. Sobald das Arbeitsverhältnis einen Auslandsbezug aufweist sind dortige nationale Regelungen zu beachten; im Übrigen gilt die DSGVO.

Übersicht über den Arbeitnehmerdatenschutz

Erlaubnistatbestände im Arbeitsverhältnis

Für die Verarbeitung von Daten im Rahmen des Beschäftigungsverhältnisses müssen nach § 26 BDSG gewisse Voraussetzungen erfüllt sein, damit die Verarbeitung rechtmäßig ist. Hierfür hat der Gesetzgeber folgende **Erlaubnistatbestände** aufgestellt:



Übersicht über den Arbeitnehmerdatenschutz

Erlaubnistatbestände im Arbeitsverhältnis

Erlaubnistatbestand: Erforderlichkeit (§ 26 Abs. 1 BDSG)

Die Verarbeitung von Daten ist gerechtfertigt, wenn dies zur **Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich** ist.

Maßstab der Erforderlichkeit:

- **Legitimer Zweck** (z.B. Meldung an das Finanzamt)
- **Geeignetheit** – Ist dem verfolgten Zweck dienlich
- **Erforderlichkeit** – Mildestes zur Verfügung stehendes Mittel
- **Angemessenheit** – Abwägung und Vergleich der schutzwürdigen Interessen

Sonderfall ist die Erhebung, Verarbeitung oder Verwendung von Daten zur **Aufdeckung von Straftaten** im Rahmen des Arbeitsverhältnisses (§ 26 Abs. 1 S. 2 BDSG). Hierfür sind tatsächliche Anhaltspunkte dafür notwendig, dass eine Straftat begangen wurde (BAG, 20.10.2016, NJW 2016, 1179). **Überwachungsmaßnahmen zu präventiven Zwecken** fallen unter § 26 Abs. 1 S. 1 BDSG.

Erlaubnistatbestand: Einwilligung (§ 26 Abs. 2 BDSG)

Grundsätzliche Anforderungen (Art. 7 DSGVO)	• **Nachweis** über die Einwilligung obliegt dem Arbeitgeber (Abs. 1) • Ausdrücklicher Hinweis auf die **Widerrufsmöglichkeit** und den **Verantwortlichen** (Abs. 3) • Einwilligung muss **freiwillig, bestimmt, informiert und unmissverständlich** den Willen zum Ausdruck bringen (Art. 4 Nr. 11 DSGVO) • **Koppelungsverbot**: Einwilligung ist unzulässig, falls die Vertragserfüllung ohne Daten-verwendung möglich ist (Abs. 4)
Besondere Anforderungen (§26 II BDSG)	• Grundsätzlich **nur in Schriftform oder elektronisch** (Ausnahme: „besondere Umstände“). • Aufklärung über den **Zweck der Datenerhebung** in Textform. • **Schwerpunkt Freiwilligkeit**: Freiwilligkeit liegt regelmäßig vor, wenn (auch) der AN einen Vorteil erlangt oder zumindest gleichgerichtete Interessen (z.B. Geburtstagsliste) verfolgt werden.

Übersicht über den Arbeitnehmerdatenschutz

Rolle des Betriebsrats

Eigene datenschutzrechtliche Verantwortlichkeit:

Zunächst war nach Einführung der DSGVO strittig, ob den Betriebsrat eigene Verantwortlichkeiten und Verpflichtungen treffen, wenn er im Rahmen seiner Tätigkeit Arbeitnehmerdaten verarbeitet. Die aktuelle Bundesregierung hat im Betriebsrätemodernisierungsgesetz von 2021 im neuen § 79a BetrVG festgeschrieben, dass den Betriebsrat **keine eigene Verantwortlichkeit** trifft.

Mitwirkung des Betriebsrats beim Arbeitnehmerdatenschutz:

Bei der Ausübung der folgenden gesetzlichen Rechte kann der Betriebsrat beim Arbeitnehmerdatenschutz mitwirken:

Mitwirkung bei Personalfragebögen nach § 94 BetrVG oder bei persönlichen Angaben in Arbeitsverträgen (§ 94 Abs. 2 BetrVG).

Aufstellung von Grundsätzen für die Personalplanung nach § 92 Abs. 1 BetrVG

Aufstellung allgemeiner Beurteilungsgrundsätze nach § 94 Abs. 2 BetrVG

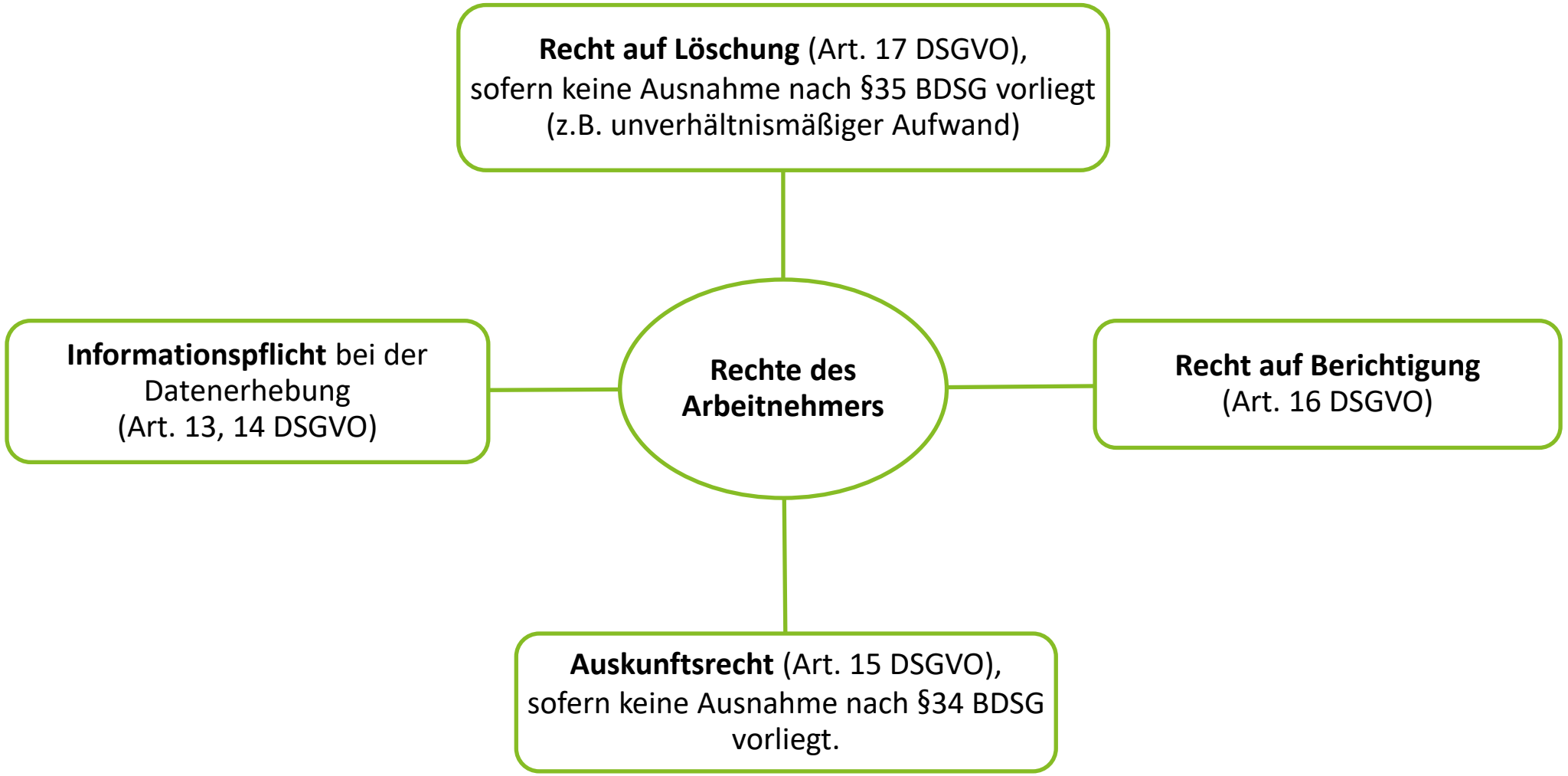
Allgemeiner Auskunfts- und Unterrichtungsanspruch aus § 80 Abs. 2 BetrVG: Hierfür muss eine Aufgabe des Betriebsrat betroffen sein und eine Auskunft zur Wahrnehmung der Aufgabe erforderlich sein.

Auswahlrichtlinien (§ 95 BetrVG) bei Einstellung, Versetzung oder Umgruppierung

Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG: Zwingendes Mitbestimmungsrecht bei jeder technischen Einrichtung, die objektiv zur Überwachung des Arbeitnehmers geeignet ist.

Übersicht über den Arbeitnehmerdatenschutz

Rechte der Arbeitnehmer



Umgang mit Bewerberdaten

Datenerhebung im Auswahlprozess

Ausschreibung, Bewerbung:

Antwortet ein Bewerber auf eine Stellenausschreibung, erhebt der potentielle Arbeitgeber personenbezogene Bewerberdaten. Grundsätzlich wird die Verarbeitung **erforderlich** sein, wenn nicht schon eine konkludente Einwilligung des Arbeitnehmers vorliegt.

Unabhängig davon muss der Arbeitgeber jedoch in jedem Fall seinen gesetzlichen Informationspflichten nachkommen und dem Arbeitnehmer **bereits in der Stellenausschreibung** die Datenerhebung mitteilen (Art. 14 DSGVO). In einem **digitalen Bewerbungsportal** sollten die entsprechenden Datenschutzhinweise vollständig akzeptiert werden, bevor die Bewerbung abgeschickt wird (optimalerweise bereits bei Registrierung im Portal).

Fragerechte des Arbeitgebers:

Im Rahmen des Auswahlprozesses wird der Arbeitgeber spätestens im Vorstellungsgespräch mehr über den Arbeitnehmer erfahren wollen. Grundsätzlich zulässig sind dabei Fragen nach leistungsbezogenen Eigenschaften des Arbeitnehmers (Ausbildung, Fähigkeiten, bisherige Arbeitsstellen).

Das Datenschutzrecht stellt hier regelmäßig keine Grenzen auf, da der Arbeitnehmer Preis geben darf was er möchte (Einwilligung). Stattdessen muss der Arbeitgeber beachten, dass er keine diskriminierenden Fragen i.S.d. AGG stellt (Schwangerschaft, Schwerbehinderung, Familienstand, Gewerkschaftszugehörigkeit, politische Einstellung, Rauchereigenschaft, Religionszugehörigkeit, usw.).

Sofern der Arbeitnehmer kein „Recht zur Lüge“ bei unzulässigen Fragen hat, gilt als Konsequenz für relevante Falschaussagen: Der Arbeitgeber kann im Fall einer **arglistigen Täuschung** das Arbeitsverhältnis anfechten, wobei die Anfechtung nicht rückwirkend das Arbeitsverhältnis auflöst, sondern **nur in die Zukunft** wirkt (BAG, NJW 1958, 516).

Background-Checks:

→ **LAG Baden-Württemberg, ZD 2020, 50**: *„Ein Background-Check bei **frei zugänglichen Quellen, u.a. im Internet**, ist bei einem Arbeitnehmer im Falle der Aufklärung von Unstimmigkeiten im Lebenslauf datenschutzrechtlich zulässig.“*

Im übrigen gelten hier die Vorschriften zur Arbeitnehmerüberwachung (Aufklärung von Pflichtverletzungen oder Straftaten) entsprechend, siehe dazu später.

Digitale Personaldaten

Grundlagen

Allgemeines zur Datenspeicherung beim Arbeitgeber:

Grundsätzlich gelten die **üblichen Erlaubnistatbestände** hinsichtlich der Aufnahme von Arbeitnehmerdaten in die Personalakten (Erforderlichkeit – Betriebsvereinbarung – Einwilligung).

Weil Personalakten regelmäßig sensible persönliche Informationen beinhalten, müssen besondere Sicherheitsvorkehrungen getroffen werden (§ 26 Abs. 3 S. 3 BDSG):

- **Zugriffskontrolle**: Daten dürfen nicht öffentlich zugänglich sein.
- **Bearbeitungskontrolle**: Es muss erkennbar sein, wer die Daten wann bearbeitet hat.
- **Verschlüsselung**

Dass die ordnungsgemäße Verwendung von Arbeitnehmerdaten im Betriebsalltag Herausforderungen begründet – und regelmäßig auch das aktive Einverständnis des Arbeitnehmers erfordert – zeigen die folgenden Beispiele:

Beispiel: Biometrisches Zeiterfassungssystem (Fingerabdruck beim Stempeln)

→ **LAG Berlin-Brandenburg, NZA 2020, 457:** Grundsätzlich ist die Arbeitszeiterfassung mithilfe von personenbezogenen Merkmalen unbeschränkt zulässig, jedoch **sind biometrische Daten besonders schützenswert** (Art. 9 DSGVO), so dass der Arbeitgeber hierauf **nicht ohne Einwilligung** zurückgreifen darf.

Beispiel: Betriebliches Eingliederungsmanagement

→ **BAG, NZA 2019, 1355**: Will der Arbeitgeber das betriebliche Eingliederungsmanagement durchführen, muss der Arbeitnehmer zuvor umfassend bei seiner **Einwilligung** auf die erhobenen Gesundheitsdaten hingewiesen werden (§ 84 II 2 SGB IX). Unterlässt er dies, so kann er bei Ablehnung des Arbeitnehmers sich nicht darauf berufen keine betriebliches Eingliederungsmanagement mehr anbieten zu müssen.

Digitale Personaldaten

Austausch im Konzern/mit Dritten

Sollen Arbeitnehmerdaten mit anderen Konzernunternehmen geteilt werden, so **gelten die allgemeinen datenschutzrechtlichen Regelungen**; ein mögliches „Konzernprivileg“ kennt das Datenschutzrecht nicht. Es ist zu unterscheiden, aus welchem Grund die Daten an andere Personen übermittelt werden:

- **Auftragsdatenverarbeitung (Art. 28 DSGVO)**: Hierbei werden Arbeitnehmerdaten im Rahmen eines Auftrages an einen Dritten weitergegeben. Der Auftrag kann bspw. Entgeltabrechnung für die Arbeitnehmer oder die Abwicklung einer Geschäftsreise durch einen Reisedienstleister sein. In diesem Fall müssen nur die Sicherheitsstandards der DSGVO eingehalten werden; Erlaubnistatbestände müssen nicht gesondert vorliegen.
- **Datenübermittlung**: Hier sind alle anderen Vorgänge gemeint, bei denen Daten zwischen verschiedenen Personen geteilt werden. Im Konzern kommt dafür bspw. die Führung einer einheitlichen Mitarbeiterkontaktliste oder die zentrale Personalplanung in Frage.

  Hierbei ist stets auf die **allgemeinen Erlaubnistatbestände** (Erforderlichkeit, Betriebsvereinbarung, Einwilligung) zu achten, wobei sich der Arbeitgeber auch auf **ein „berechtigtes Interesse“ bei der Weiterleitung im Konzern** berufen kann. Eine berechtigtes Interesse liegt unter anderem vor bei:

  - Entsendungen an das Konzernunternehmen
  - Inanspruchnahme von konzernweiten Sonderleistungen
  - Konzernweites Mailverzeichnis

Sitzt die andere Konzerngesellschaft oder der Dritte im **Ausland**, so gelten besondere Anforderungen:

- **In der EU**: unproblematisch zu den allgemeinen Regelungen
- **Außerhalb der EU**: Liegt keine Konformitätserklärung der EU-Kommission vor, so müssen die **speziellen Vorschriften für die Datenübermittlung ins Ausland nach Art. 44 DSGVO beachtet werden**. Hierbei ist regelmäßig eine ausdrückliche Einwilligung des Arbeitnehmers notwendig.

Digitales Corona-Management

Allgemeines zur Behandlung von Gesundheitsdaten:

Informationen über den Gesundheitszustand des Arbeitnehmers sind besonders vertraulich zu behandeln; sie gelten als **personenbezogene Daten besonderer Kategorien** (Art. 9 DSGVO). Dementsprechend sind grundsätzlich alle medizinischen Angaben (z.B. Krankmeldungen, Betriebsuntersuchungen) entsprechend zu schützen:

- **Zugriffskontrolle**: Daten dürfen nicht öffentlich zugänglich sein.
- **Bearbeitungskontrolle**: Es muss erkennbar sein, wer die Daten wann bearbeitet hat.
- **Verschlüsselung**

Wiederum gelten die allgemeinen Voraussetzungen für die Verarbeitung von Arbeitnehmerdaten.

Gesundheitsstatus im Zusammenhang mit COVID-19:

- **Impfpflicht im Betrieb:** Grundsätzlich müssen sich Arbeitnehmer noch nicht verpflichtend impfen lassen. Der Arbeitgeber kann keine Impflicht anordnen.
- **Frage nach Impfung/Genesung?**: Kann der Arbeitgeber ein berechtigtes Interesse an dieser Frage nachweisen (z.B. bei Kundenkontakt im Betrieb), so kann sich der Auskunftsanspruch des Arbeitgeber aus dem Erlaubnistatbestand „Erforderlichkeit“ ergeben.
- **Testpflicht im Betrieb**: Entsprechend § 4 der Corona-Arbeitsschutzverordnung muss der Arbeitgeber wöchentlich mindestens 2 Corona-Tests anbieten; eine Testpflicht außerhalb des Gesundheitssektors besteht jedoch nicht.

Neues zum Entgeltfortzahlungsanspruch:

Ab 01.11.2021 entfällt bundesweit der gesetzliche Entgeltfortzahlungsanspruch für Personen, die mangels Impfung oder Genesung in Quarantäne müssen. In Baden-Württemberg gilt die entsprechende Regelung seit dem 15.09.2021, in Rheinland-Pfalz seit dem 01.10.2021.

Überwachung von Arbeitnehmern

Allgemeines

Klassische Überwachung:

Zwar werden durch § 26 Abs. 1 S. 2 BDSG Überwachungsmaßnahmen des Arbeitgebers bei „tatsächlichen Anhaltspunkte“ für den Verdacht einer „Straftat“ ermöglicht, nach der Rechtsprechung des BAG kann der Arbeitgeber jedoch nach § 26 Abs. 1 S. 1 BDSG schon Überwachungsmaßnahmen beim **Verdacht einer „schwerwiegenden Pflichtverletzung“** vornehmen. Klassische Überwachungsmaßnahmen sind beispielsweise Videoüberwachung, Einlasskontrollen oder Detektivermittlungen.

Ausnahmefälle:

- **Präventive Überwachung** im Betrieb, die sich **nicht an Arbeitnehmer richtet** (z.B. Sicherung von Anlagen, Arbeitssicherheit), ist grundsätzlich möglich.
- **Öffentliche Betriebsflächen** (z.B. Verkaufsraum) dürfen z.B. zum Schutz vor Diebstahl grundsätzlich überwacht werden.
- **Private Rückzugsflächen sind jedoch von jeder Überwachung ausgenommen** Der Arbeitgeber darf in bestimmten Bereichen überhaupt keine Überwachung durchführen, weil dies das Persönlichkeitsrecht des Arbeitnehmers zu stark einschränken würde (bspw. Toilette oder Umkleide).

Durchführungstipps:

- Über eine Überwachung muss stets entsprechend der Vorgaben der DSGVO transparent **informiert** werden.
- Die Anlasspunkte für einen Verdacht einer Straftat oder schwerwiegenden Pflichtverletzung sind stets unter Nennung des Datums zu **dokumentieren**.
- Konkrete Ermittlungsmaßnahmen sollten nicht ohne vorherigen **Rechtsbeistand** durchgeführt werden.

Mitbestimmungsrecht:

Eine **technische Überwachungseinrichtung** begründet ein Mitbestimmungsrecht des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG). Nach st. Rspr. des BAG ist eine technische Überwachungseinrichtung jede Einrichtung, die sich objektiv zur Überwachung von Arbeitnehmern eignet (zurückgehend auf BAG, NJW 1976, 261).

Überwachung von Arbeitnehmern

Digitale Überwachung

Neue Überwachungseinrichtungen i.S.d. Mitbestimmungsrechts:

Seit der Leitentscheidung des BAG hat sich der Arbeitsplatz jedoch wesentlich digitalisiert. Eine Änderung des Mitbestimmungstatbestandes hat jedoch nicht stattgefunden, weshalb folgende Maßnahmen des Arbeitgebers bereits eine Beteiligung des Betriebsrats voraussetzen:

- **Facebook-Profil** (BAG, NZA 2017, 657) oder **Twitter-Profil** (LAG Hamburg, NZA-RR 2018, 655) des Arbeitgebers wegen Aussagen über das Arbeitsverhalten der Arbeitnehmer, die das Profil betreuen: *„Die Funktion „Besucher-Beiträge“ erlaubt derzeit den Nutzern von Facebook, Postings zum Verhalten und zur Leistung der bei den konzernzugehörigen Unternehmen beschäftigten Arbeitnehmern auf der Seite der Arbeitgeberin einzustellen. Je nach dem Inhalt dieser „Besucher-Beiträge“ können diese namentlich oder situationsbedingt einem bestimmten Arbeitnehmer zugeordnet werden*.“
- **Standardprogramme** wie **Webbrowser** (Firefox, Chrome, usw.) oder **Microsoft-Office Produkte** (so ausdrücklich für Microsoft Office Kalender: LAG Nürnberg, NZA 2017, NZA-RR 2017, 302). Das BAG betonte bei der Einordnung von **Microsoft Office Excel** als mitbestimmungspflichtiges Programm: *„Das Mitbestimmungsrecht ist darauf gerichtet, Arbeitnehmer vor **Beeinträchtigungen ihres Persönlichkeitsrechts durch den Einsatz technischer Überwachungsmaßnahmen zu bewahren**, […]..*
- Das **Betriebssystem** vom Handys oder Computern (für Microsoft 2000 damals LAG, Hamm, 10 TaBV 173/05)
- **Personalabrechnungssysteme** (BAG, NZA 1985, 669).

Überwachung von Arbeitnehmern

Beweismittelverwertung

Voraussetzungen:

Im Rahmen der Arbeitnehmerüberwachung erlangte Erkenntnisse sind (gerichtlich) verwertbar, wenn:

Datenschutzrechtliche Vorschriften eingehalten wurden (v.a. § 26 BDSG) + Nicht gegen Vorschriften aus einer **Betriebsvereinbarung** verstoßen wurde + **Keine Mitbestimmungsrechte** des Betriebsrats verletzt wurden (v.a. § 87 Abs. 1 Nr. 6 BetrVG)

Folgen bei Verstößen

Datenschutzrechtliche Vorschriften	Die Zulässigkeit von Beweisen im Prozess ist **unabhängig** von anderen Vorschriften wie § 26 BDSG, einer Betriebsvereinbarung oder eines Mitbestimmungsrechts zu bewerten. Konkret kommt es dabei auf die **Rechtfertigung des Eingriffs** in das Persönlichkeitsrechts des Arbeitnehmers durch den Arbeitgeber an (BAG, NZA 2017, 112 und BAG, NZA 2014, 243 für Videoüberwachung; BAG, NZA 2008 1008 und BAG, NZA 2003, 1193 für Mitbestimmungsrechte bzw. Betriebsvereinbarung)
Betriebsvereinbarung	
Mitbestimmungsrechte	

Achtung: Hier geht nur um die Verwertbarkeit von Beweisen. Etwaige rechtliche Konsequenzen, die der Arbeitnehmer wegen der Verletzung seiner Persönlichkeitsrechte geltend machen kann, sind unabhängig davon zu bewerten.

Data Incident Management

Vorgehen bei Datenpannen:

1) Daten umgehen sichern, Angriff abwehren.
2) Unverzügliche **Mitteilung an die zuständige Aufsichtsbehörde** – spätestens innerhalb von 72 Stunden (Art. 33 DSGVO)
   - Informationen über Ausmaß der Datenschutzverletzung
   - Drohende Folgen und Gegenmaßnahmen
   - Kontaktperson des Arbeitgebers
3) **Information der betroffenen Arbeitnehmer** nach Art. 34 DSGVO
   - Beschreibung des Vorfalls muss in „klarer und einfacher“ Sprache erfolgen
   - Selbe Inhalte wie bei der Mitteilung an die Aufsichtsbehörde

Rechtliche Konsequenzen für den Arbeitgeber:

- **Bußgelder** bei Missachtung von Datenschutzvorschriften (Art. 83 Abs. 4 DSGVO)
- **Bußgelder** bei fehlender Unterrichtung entsprechend 2) und 3)
- **Strafbarkeit** bei Datenweitergabe oder Datenverkauf
- **Schadenersatzansprüche** der betroffenen Personen

Ansprechpartner

Nathalie Polkowski (nee Nemecek)
Employment Law & Benefits
Rechtsanwältin | Fachanwältin für Arbeitsrecht
Senior Associate

Tel.: +49 89 29036 8996
Mobil: +49 151 5807 11 64
E-Mail: npolkowski@deloitte.de

Dr. Martin Döpner
Employment Law & Benefits
Rechtsanwalt
Counsel

Tel.: +49 211 8772 2089
Mobil: +49 151 5800 1288
E-Mail: mdoepner@deloitte.de

Deloitte Legal

Experience the future of law, today

Mehr als
2,500
Anwälte

in
80+
Ländern

Nahtlose Zusammenarbeit

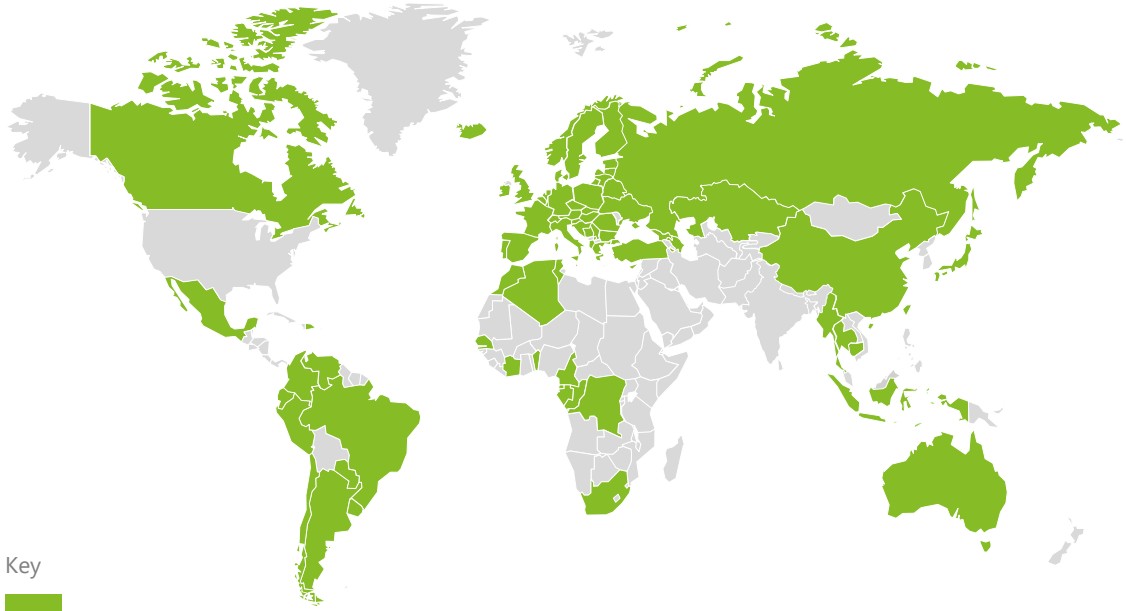
Grenzüberschreitend und mit andern Deloitte Business Lines

Als Teil des weltweiten Deloitte Professional Services Netzwerks, arbeitet Deloitte Legal eng mit Kollegen weltweit zusammen, um Mandanten eine integrierte Beratung und multinationale Lösungen zu bieten, die:

- **Konsistent** mit ihrer Unternehmensvision
- **Technologie-basiert** für eine bessere Zusammenarbeit und mehr Transparenz
- **Maßgeschneidert** auf die Unternehmensform und den lokalen Markt
- **Sensibilisiert** für die jeweiligen regulatorischen Bestimmungen

Deloitte Legal ist weltweit stark aufgestellt

Wir erbringen Rechtsberatungsleistungen in **80+** Ländern und können dank unserer Beziehungen zu hochqualifizierten Anwaltskanzleien Mandanten in knapp **150** Ländern der Welt beraten.



Deloitte Legal global coverage

Deloitte Legal practices

1. Albania
2. Algeria
3. Argentina
4. Armenia
5. Australia
6. Austria
7. Azerbaijan
8. Belarus
9. Belgium
10. Benin
11. Bosnia
12. Brazil
13. Bulgaria
14. Cambodia
15. Cameroon
16. Canada
17. Chile
18. China
19. Colombia
20. Congo, Rep. of
21. Costa Rica
22. Croatia
23. Cyprus
24. Czech Rep.
25. Dem Rep of Congo
26. Denmark
27. Dominican Republic
28. Ecuador
29. El Salvador
30. Equatorial Guinea
31. Estonia
32. Finland
33. France
34. Gabon
35. Georgia
36. Germany
37. Greece
38. Guatemala
39. Honduras
40. Hong Kong
41. Hungary
42. Iceland
43. Indonesia
44. Ireland
45. Italy
46. Ivory Coast
47. Japan
48. Kazakhstan
49. Kosovo
50. Latvia
51. Lithuania
52. Luxembourg
53. Malta
54. Mexico
55. Montenegro
56. Morocco
57. Myanmar
58. Netherlands
59. Nicaragua
60. Norway
61. Paraguay
62. Peru
63. Poland
64. Portugal
65. Romania
66. Russia
67. Senegal
68. Serbia
69. Singapore
70. Slovakia
71. Slovenia
72. South Africa
73. Spain
74. Sweden
75. Switzerland
76. Taiwan
77. Thailand
78. Tunisia
79. Turkey
80. Ukraine
81. Uruguay
82. United Kingdom
83. Venezuela

Deloitte.
Legal