RITTERWALD

Unternehmensberatung

Datenschutz bei Wohnungsgenossen-schaften – Eine wichtige Rahmen-bedingung der Digitalisierung

Eine Einführung in die DSGVO für Wohnungsgenossenschaften

Münster, 19.10.2017

RITTERWALD berät Kunden im gesamten Bundesgebiet und bietet europäisches Netzwerk – Bürostandorte in Berlin und Frankfurt

RITTERWALD Kurzportrait

DEUTSCHLAND

- **Bundesweite Beratung** von unterschiedlichen Kunden, Fokus auf der Wohnungswirtschaft
- **Bürostandorte in Berlin und Frankfurt am Main** bilden optimale Ausgangspunkte für eine deutschlandweite Präsenz

○ *Bürostandorte RITTERWALD*
● *Projektstandorte RITTERWALD*

EUROPA

- RITTERWALD ist seit 2014 Mitglied in der **European Federation for Living (EFL), mit Sitz in Amsterdam**
- Mitgliedschaft ermöglicht **internationalen Dialog** mit Unternehmen, Investoren sowie Universitäten auf dem Gebiet der Wohnungswirtschaft

Quelle: Ritterwald

Aufsichtsbehörden und Gerichte treffen regelmäßig spezifische Entscheidungen und Urteile für die Wohnungswirtschaft

Beispiele spezifischer Entscheidungen

Die Verarbeitung mieterbezogener Daten ist im Bewerberverfahren nur beschränkt möglich. So kann z.B. die ein Nachweis über die Höhe des Einkommens erst dann abgefragt werden, wenn die Entscheidung über den Mieter bereits gefallen ist

Orientierungshilfe vom Düsseldorfer Kreis –, 27.01.2014

Die Installation von smart-home Sensoren, die Luftfeuchtigkeit, Temperatur, Luftdruck und CO_2 Ausstoß messen, ist nur erlaubt, wenn der Mieter seine Einwilligung erteilt

Aufsichtsbehörde des Saarlandes, Report 2015/16, S.169

Die Installation von Videokameras oder Attrappen im Eingangsbereich eines Mehrfamilienhauses ist verboten und erfordert die Zustimmung aller Mieter

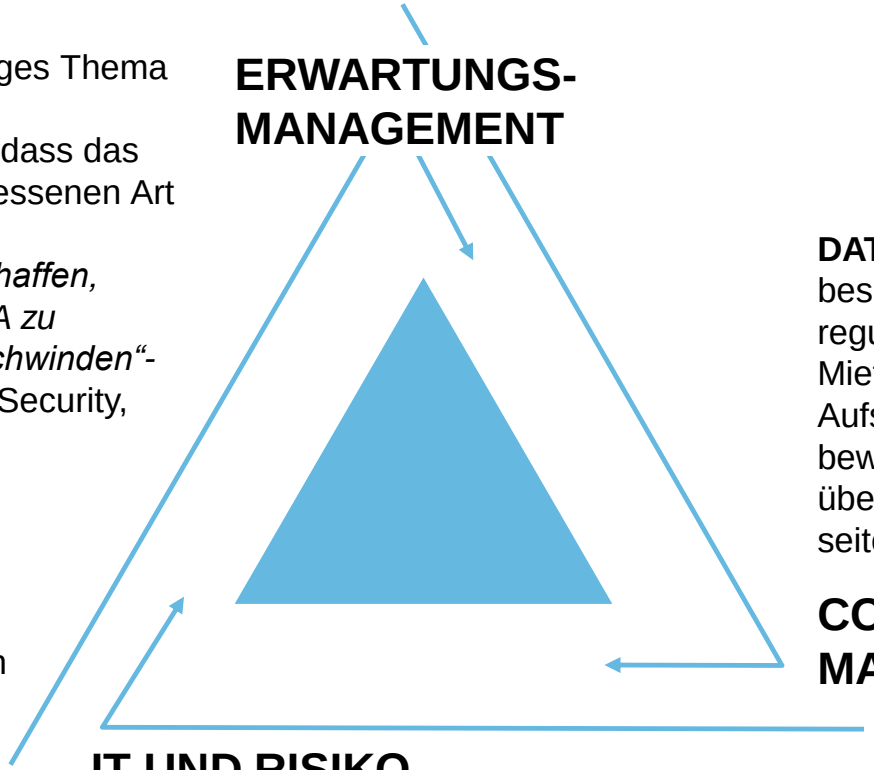
AG Frankfurt, 29.1.2015, 33 C 3407/14

Datenschutz betrifft Unternehmen in vielen Bereichen – Unternehmen sollten dies in ihrer Strategie berücksichtigen

Bedeutung des Datenschutzes für Unternehmen

DATENSCHUTZ ist ein wichtiges Thema für Kunden, Angestellte und Gesellschafter. Alle erwarten, dass das Unternehmen in einer angemessenen Art und Weise mit Daten umgeht.
„Unternehmen die es nicht schaffen, Datenschutz als Teil ihrer DNA zu implementieren, werden verschwinden“- Daryl Pereira, Head of Cyber Security, KPMG/Singapur

DATENSCHUTZ erfordert den Schutz vor Datenpannen. Andernfalls drohen hohe indirekte und direkte finanzielle Schäden.



DATENSCHUTZ wird in der EU besonders stark gefordert und reguliert. Die Verarbeitung von Mieterdaten wird von den Aufsichtsbehörden kritisch bewertet und erfordert überzeugende Argumente seitens der Unternehmen

Quelle: Ritterwald

Die EU-Kommission bemisst Datenschutz einen hohen Stellenwert ein – Unternehmen müssen sich auf die DSGVO einstellen

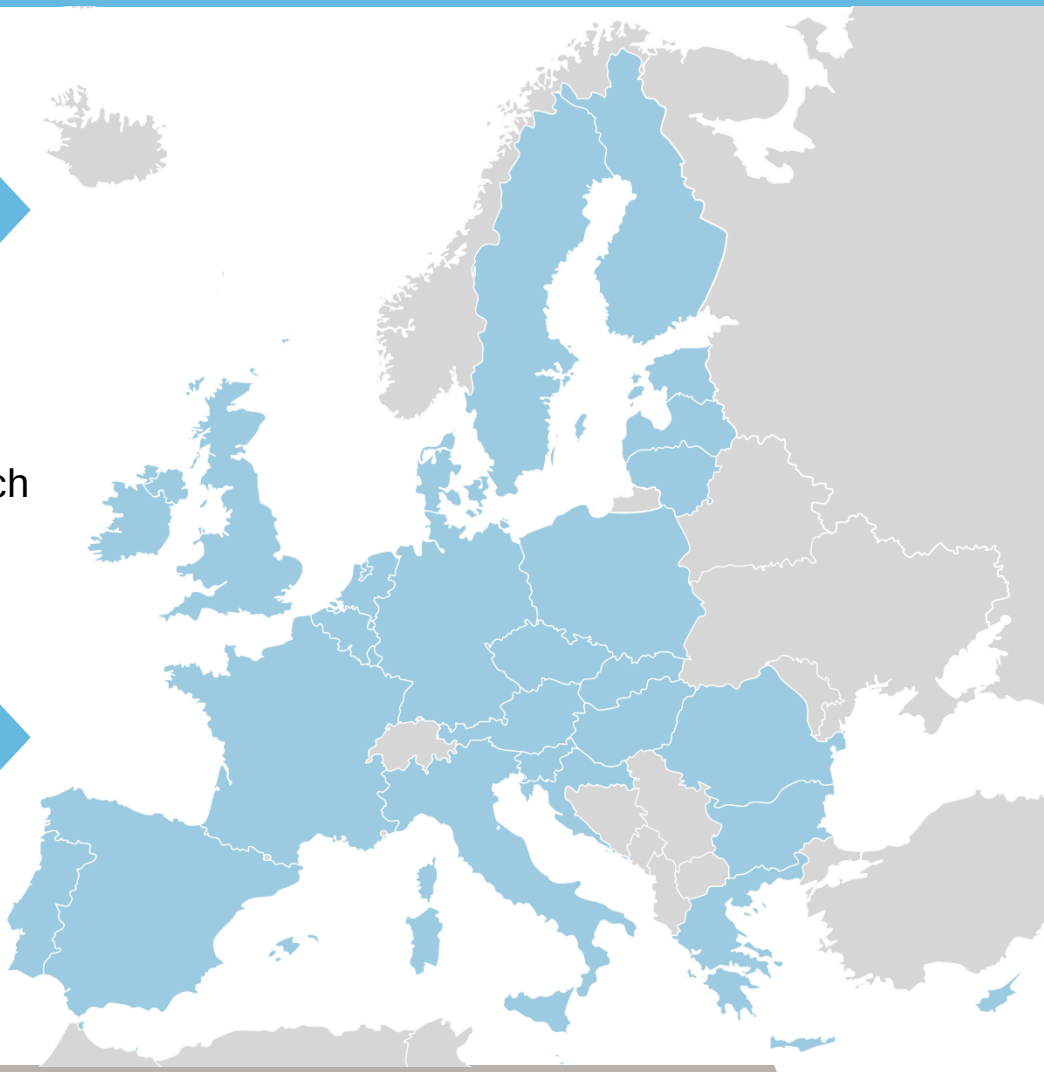
Rechtliche Rahmenbedingen in der EU

VORSCHRIFTEN SEIT 1995

- **Datenschutzrichtlinie (DSRL)** 95/46/EG (24.10.1995) betreffend der Verarbeitung personenbezogener Daten
- **Datenschutzrichtlinie für elektronische Kommunikation** 2002/58/EG (12.07.2002) auch bekannt als E-Privacy Richtlinie, die Mindestvorgaben für den Datenschutz in der Telekommunikation setzt

VORSCHRIFTEN AB 25. MAI 2018

- **Datenschutzgrundverordnung (DSGVO)** EU 2016/679 (26.04.2016) ersetzt die DSRL
- **ePrivacy Verordnung** (Entwurfsstadium) ersetzt die E-Privacy Richtlinie



Quelle: Ritterwald

Die DSGVO wurde beschlossen, um den Datenschutz in Europa zu stärken und weiter zu harmonisieren als bislang durch die DSRL

Grundsätzliche Veränderungen des Datenschutz-Rechtsrahmens

DATENSCHUTZRICHTLINIE (DSRL)

- Richtlinien definieren einen **Mindeststandard** und sind nur ihrem **Ziel** nach für die Mitgliedstaaten verbindlich
- Die einzelnen Mitgliedstaaten müssen die Richtlinie **in nationales Recht umsetzen** und haben dabei einen Spielraum
- Trotz angestrebter Harmonisierung kam es zu einem **uneinheitlichen Datenschutzniveau** in Europa

DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

- Verordnungen finden als **unmittelbar geltendes Recht** Anwendung in jedem Mitgliedstaat
- Die DSGVO beinhaltet 99 Artikel und über **60 Öffnungsklauseln –** Mitgliedstaaten können in einzelnen Bereichen Vorschriften erlassen
- Datenschutzrecht wird zwar a priori nur aus der DSGVO bestehen, aber wahrscheinlich auch aus **Vorschriften der Mitgliedstaaten**

Quelle: Ritterwald

Im Folgenden werden die wichtigsten Bestimmungen der DSGVO besprochen – Unternehmen müssen auf diese vorbereitet sein

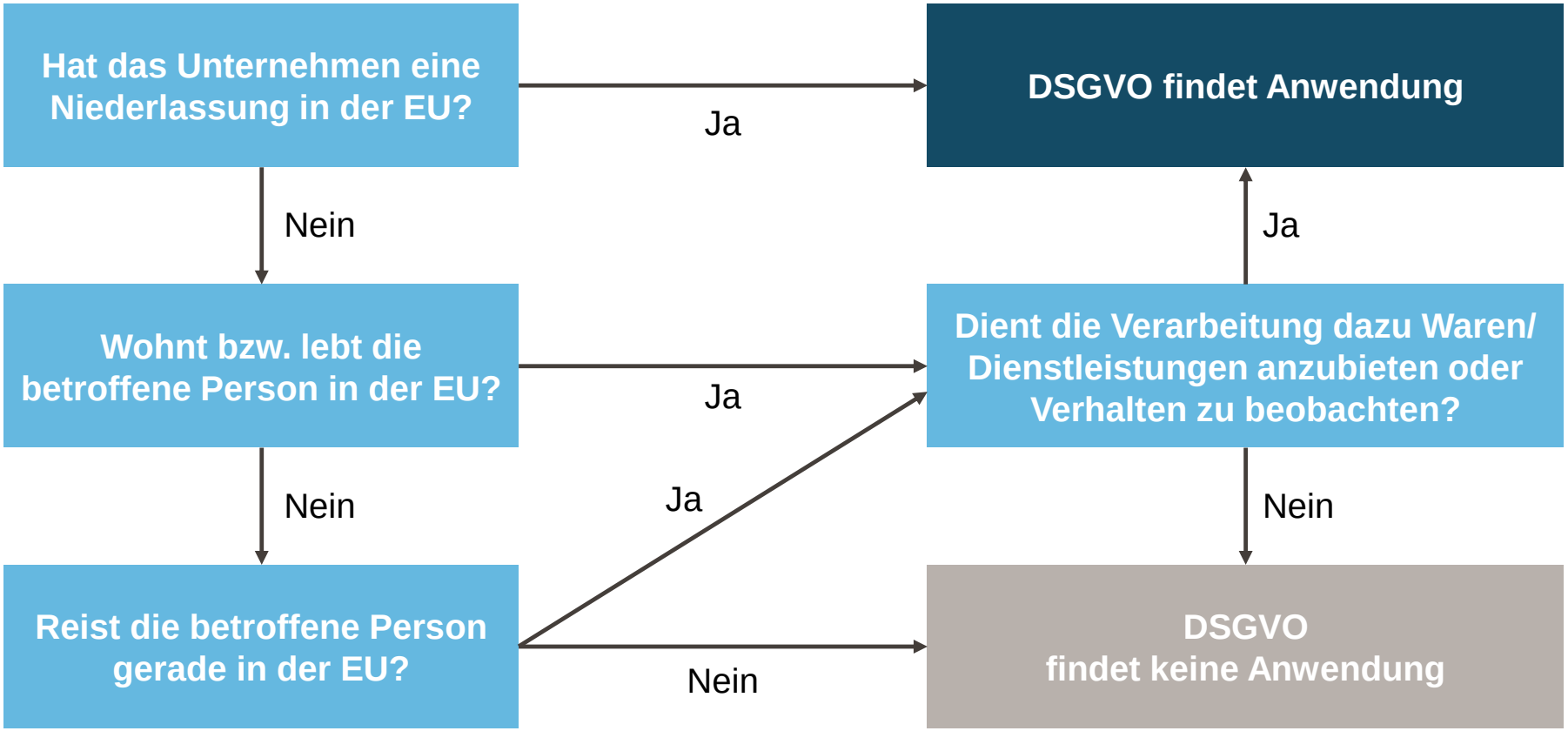
Wichtige Bestimmungen der DSGVO

1. Räumlicher Anwendungsbereich
2. Materieller Anwendungsbereich
3. Grundsätze der Datenverarbeitung
4. Datenverarbeitung
5. Auftragsverarbeitung
6. Informationspflichten
7. Betroffenenrechte
8. Datenschutz und Datensicherheit
9. Datenschutzbeauftragte
10. Haftung und Strafen

Quelle: Ritterwald

Die DSGVO erweitert den räumlichen Anwendungsbereich und betrifft alle Unternehmen die Daten von EU-Bürgern verarbeiten

Räumlicher Anwendungsbereich der DSGVO (Art. 3)



Quelle: Ritterwald

Die DSGVO erweitert den räumlichen Anwendungsbereich und betrifft alle Unternehmen die Daten von EU-Bürgern verarbeiten

Quelle: Ritterwald

Unternehmen müssen bei der Verarbeitung personenbezogener Daten nach wie vor die Grundsätze des Art. 5 DSGVO beachten

Quelle: Ritterwald

Die Verarbeitung personenbezogener Daten kann zumindest bei der Vermietung nicht auf eine Einwilligung gestützt werden

Rechtmäßigkeit der Verarbeitung – Einwilligung als Erlaubnis (Art. 6 DSGVO)

Transparenz

Betroffene Personen müssen vor Erteilung der Einwilligung umfassend informiert werden und Unternehmen müssen in der Lage sein, die Erteilung der Einwilligung nachzuweisen

Recht auf Widerruf

Betroffene Personen müssen auf ihr Widerrufsrecht hingewiesen werden

Form

Die Einwilligung kann in jeder (schriftlichen) Form also auch elektronisch erfolgen; bislang musste sie in Schriftform erfolgen

Freiwilligkeit der Einwilligung

Die Einwilligung ist nur wirksam, wenn sie freiwillig erfolgt – Die Aufsichtsbehörden verneinen dies zumindest bei der Wohnraummiete, denn der Vermieter habe eine überlegene Stellung

Die Verarbeitung personenbezogener Daten kann jedoch auf einen gesetzlichen Erlaubnistatbestand gestützt werden

Rechtmäßigkeit der Verarbeitung aufgrund rechtlicher Erlaubnis (Art. 6 DSGVO)

Verarbeitung erforderlich ...

für die Erfüllung eines Vertrags

Z.B. in Vorbereitung eines Mietvertrages

Eine rechtliche Erlaubnis genügt nicht, es muss sich um eine rechtliche Verpflichtung handeln

für die Erfüllung einer rechtlichen Verpflichtung

Verarbeitung erforderlich ...

Verarbeitung erforderlich ...

zum Schutz natürlicher Personen oder Erfüllung einer öffentlichen Aufgabe

Die Verarbeitung ist zulässig, um lebenswichtige Interessen der betroffenen Person zu schützen oder Aufgabe zu erfüllen, die im öffentlichen Interesse liegt

Die Verarbeitung ist zulässig zur Wahrung berechtigter Interesse des Verantwortlichen, sofern nicht die Interessen der betroffenen Person überwiegen

zur Wahrung berechtigter Interessen des Betroffenen

Verarbeitung erforderlich ...

Quelle: Ritterwald

Unternehmen müssen überprüfen, ob sie personenbezogene Daten in Übereinstimmung mit der DSGVO verarbeiten

Datenverarbeitung – Wichtige Hinweise

Zweckbindung – Art. 6 (4)	• Zweckbindung bedeutet, dass personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen • Verantwortliche dürfen Daten für andere Zwecke verarbeiten, wenn diese Verarbeitung mit dem ursprünglichen Zweck in Einklang steht
Verarbeitung von Kindesdaten und besonderer Kategorien – Art. 8, 9	• Die allgemeinen Verarbeitungsregeln greifen nur gegenüber betroffenen Personen, die mindestens 16 Jahre alt sind; Andernfalls müssen Eltern eine Einwilligung erteilen • Die Verarbeitung besonderer Datenkategorien ist grundsätzlich untersagt – hierzu gehören z.B. Daten aus denen die ethnische Herkunft, weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen
Wirksamkeit bisheriger Einwilligungen – Erwägungsgrund Nr. 171	• Die Erteilung einer erneuten Einwilligung ist nicht erforderlich

Quelle: Ritterwald

Für Verarbeitungen durch Dritte, im Konzern und im Ausland gelten besondere Regelungen

Regelung der Auftragsverarbeitung

NATIONALE AUFTRAGSVERARBEITER

- Erhalten Daten und verarbeiten diese im Auftrag des Verantwortlichen; werden nicht mehr als Teil des Verantwortlichen betrachtet
- Haben eigene Pflichten daher weiterhin Abgrenzung zur Funktionsübertragung erforderlich (z.B. Makler) also zu eigenständigen Verantwortlichen
- Die Auftragsverarbeitung unterliegt dem allgemeinen Verbot mit Erlaubnisvorbehalt und erfordert somit einen Vertrag zur Auftrags-verarbeitung sowie eine Einwilligung oder einen gesetzlichen Rechtfertigungsgrund

VS

INTERNATIONALE AUFTRAGSVERARBEITER

- Übertragungen zu Verarbeitern in EU-Mitgliedstaaten sind zu behandeln wie nationale Verarbeitungen
- Übertragungen in Drittländer sind nur zulässig, wenn sie den Anforderungen einer zweistufigen Legitimations-Prüfung standhalten

! Vertrag über Auftragsverarbeitung sowie Einwilligung oder gesetzlicher Rechtfertigungsgrund

! Nachweis eines angemessenen Datenschutzniveaus im Empfängerland

Quelle: Ritterwald

Unternehmen müssen sich über weitreichende Informations-pflichten bewusst werden

Übersicht der Informationspflichten

Wenn Daten bei der betroffenen Person erhoben werden – Art. 13

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- Dauer, für die die personenbezogenen Daten gespeichert werden
- Bestehen von Rechten wie z.B. Auskunftsrecht

Wenn Daten nicht bei der Person erhoben wurden – Art. 14

Informationspflichten des Art. 13 und zusätzlich:

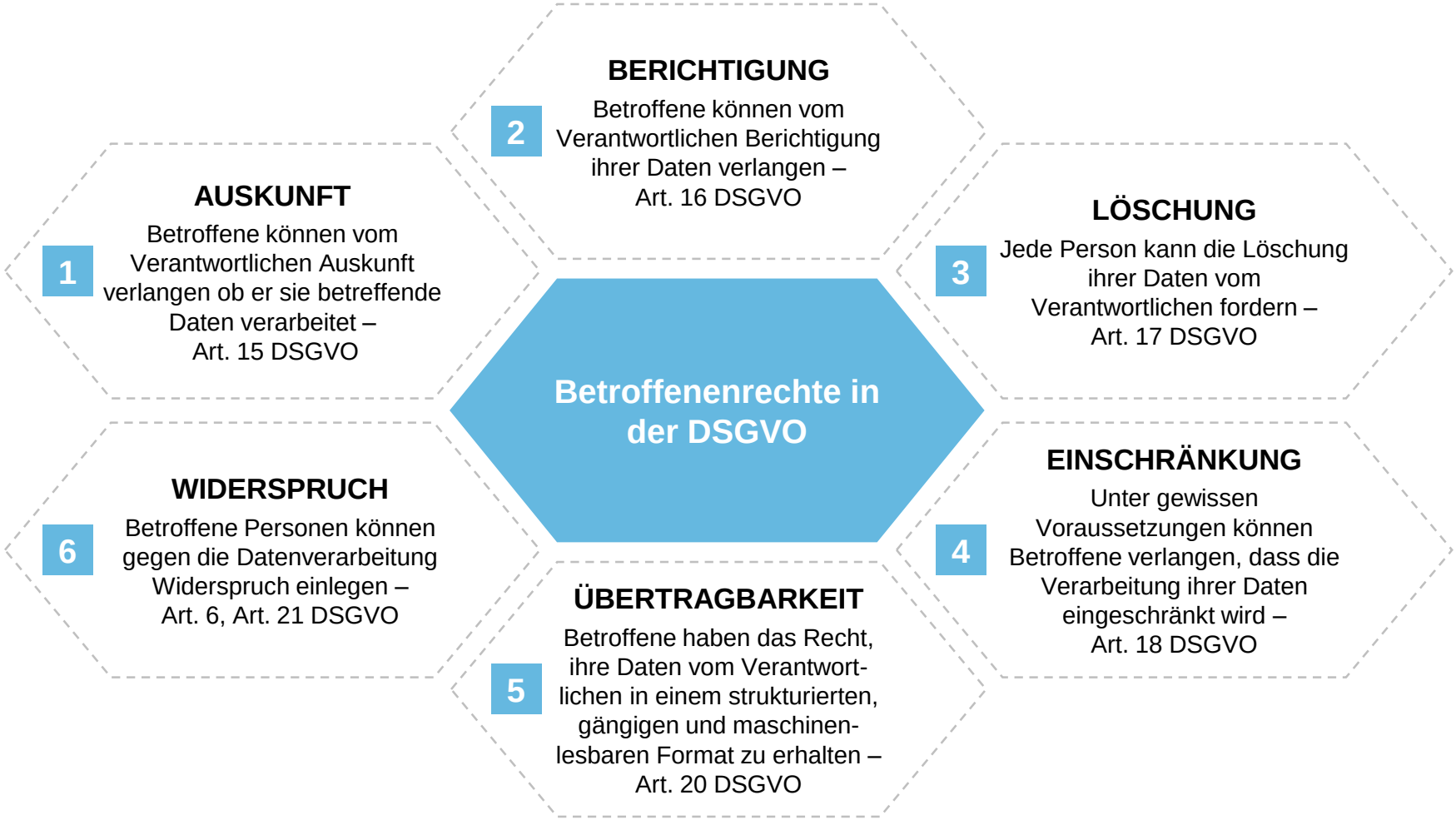
- Kategorien des betroffenen personenbezogenen Daten
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen

Meldung bei Datenschutz-verstößen Art. 33, 34

- An zuständige Aufsichtsbehörde innerhalb von 72 Stunden
- Wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht

Quelle: Ritterwald

Die bestehenden Betroffenenrechte werden durch die DSGVO präzisiert und ausgeweitet



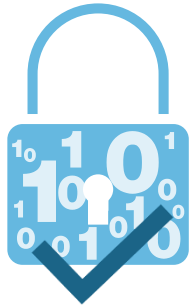
Quelle: Ritterwald

Unternehmen sind verpflichtet höhere Sicherheitsstandards durch technische und organisatorische Maßnahmen zu schaffen (TOM)

Datenschutz und Datensicherheit (1)

DATENSCHUTZ by design and by default Art. 25

- **Privacy by design** bedeutet Datenschutz durch Einsatz datenschutzfreundlicher Techniken. Als Beispiele zählt die DSVO Pseudonymisierung auf
- **Privacy by default** bedeutet den Einsatz datenschutzfreundlicher Voreinstellungen. Mit anderen Worten muss für den gesamten Lebenszyklus ein datensparsames Vorgehen in den Prozessen implementiert werden



SICHERHEIT der Verarbeitung Art. 32

- **Verantwortliche und Verarbeit**er müssen angemessene technische und organisatorische Maßnahmen schaffen, um das Risiko von Datenschutzverletzungen zu minimieren (z.B. Verschlüsselungen)
- Weitere TOM (technische und organisatorische Maßnahmen) können Zugangskontrolle, Weitergabekontrolle, Eingabekontrolle etc. sein
- Die praktische Umsetzung kann durch Einführung eines Datensicherheitsmanagements erfolgen, basierend auf anerkannten IT-Sicherheitsstandards wie z.B. ISO 27001

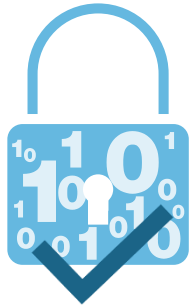
Quelle: Ritterwald

Unternehmen sind verpflichtet höhere Sicherheitsstandards durch technische und organisatorische Maßnahmen zu schaffen (TOM)

Datenschutz und Datensicherheit (2)

DATENSCHUTZ-FOLGENABSCHÄTZUNG Art.35

- Die DSGVO ersetzt die bisherige Vorabkontrolle durch die Folgenabschätzung; eine Folgenabschät-zung muss für jeden Prozess erfolgen aus dem sich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen ergeben kann
- Beispiel: systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet oder Überwachung öffentlicher Bereiche
- Die Aufsichtsbehörden werden eine Liste von Verarbeitungsvorgängen erstellen, für die eine Folgenabschätzung erforderlich ist



VERARBEITUNGSVERZEICHNIS Art.30

- Die DSGVO modifiziert die Regelungen des BDSG zum Verfahrensverzeichnis; das bisherige System vom Meldepflicht und Verfahrens-verzeichnis wird durch die in Art. 30 normierten Aufzeichnungspflichten abgelöst
- Die bisherigen Befreiungen des BDSG (z.B. bei Bestellung eines DSB) gelten nicht. Die Ausnahme für Betriebe bis 250 Mitarbeiter wird häufig an der Rückausnahme der „nur gelegentlichen Verarbeitung“ scheitern
- Das Verarbeitungsverzeichnis sollte Informationen enthalten über Name und Kontaktdaten des Verantwortlichen, Zweck der Verarbeitung, Kategorien betroffener Personen und personenbezogener Daten etc.

Quelle: Ritterwald

Die Bestellung eines Datenschutzbeauftragten wird verpflichtend für einige Unternehmen

Datenschutzbeauftragte (Art. 37)

BESTELLUNG

- Grundsätzlich besteht keine Verpflichtung zur Bestellung eines DSB aber nationales Recht kann hiervon Ausnahmen vorsehen
- Ein DSB muss z.B. bestellt werden, wenn die Kerntätigkeit in der Durchführung von Verarbeitungen besteht

STATUS

- Er muss ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden
- DSBs müssen qualifiziert und unabhängig sein und direkt an die höchste Managementebene reporten

DPO – Art. 37ff.

AUFGABEN

- DSB informieren und beraten den Verantwortlichen im Unternehmen und die Angestellten
- **Weitere Aufgaben können zwischen dem DSB und dem Verantwortlichen abgemacht werden**
- **Sie achten auf die Einhaltung des Datenschutzes**

HAFTUNG

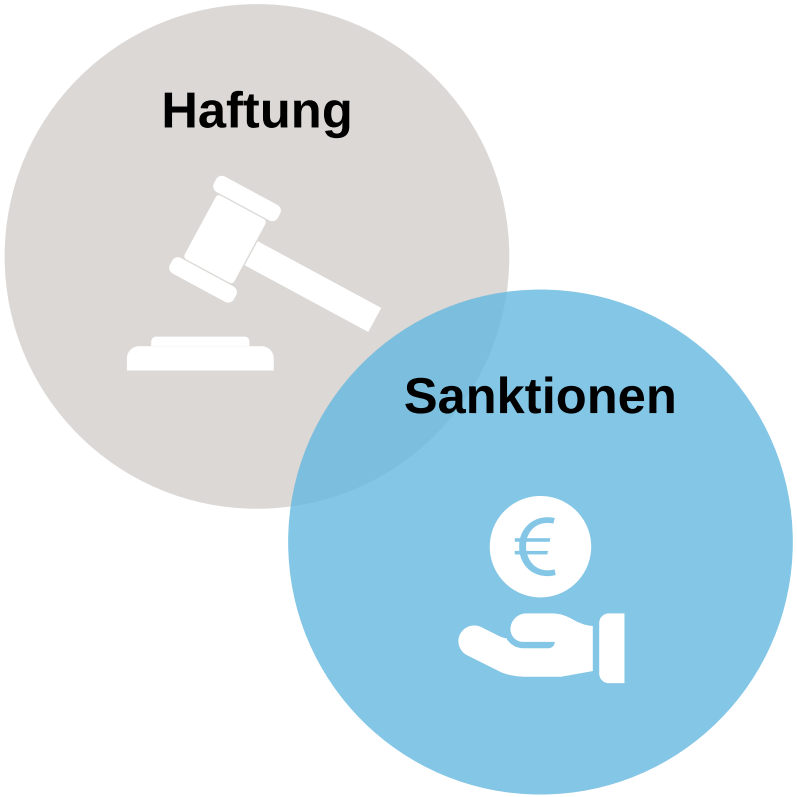
- Die DSGVO sieht keine direkte Haftung des DSB vor allerdings kann er durch Verantwortliche oder Auftragsverarbeiter haftbar gemacht werden im Fall von Pflichtverletzungen
- Interne DSB haften nur für Fahrlässigkeit, externe DSB haften auch für einfache Fahrlässigkeit

Quelle: Ritterwald

Unternehmen müssen sich darüber bewusst sein, dass die DSGVO erhebliche Sanktionen vorsieht

Haftung und Strafen – Art. 82,83

Jede Person die einen materiellen oder immateriellen Schaden erleidet, kann Schadensersatz dafür fordern, wenn dieser Schaden durch eine Verletzung der DSGVO entstanden ist



- Aufsichtsbehörden haben eine Vielzahl von Untersuchungs- und Abhilfebefugnissen und können zusätzlich Geldbußen verhängen
- Geldbußen können bis zu 20 Mio. Euro oder 4% des weltweiten Umsatzes betragen

Quelle: Ritterwald

Umsetzung von Datenschutz-Compliance setzt Kenntnisse und Verständnis der DSGVO voraus

Übersicht zu den wichtigsten Regelungen der DSGVO

1	Rechtmäßigen Umgang mit Daten nachweisen (Art. 5 und 6)	
Rechtmäßigkeit, Transparenz	Zweckbindung	Datensparsamkeit
Richtigkeit	Speicher-begrenzung	Integrität und Vertraulichkeit

2	Durch TOM[1)] die Verarbeitung in Übereinstimmung mit der DSGVO garantieren (Art. 24)	
Datenschutz by design & default (Art. 25)	Auftragsverarbeiter (Art. 28)	Sicherheit der Verarbeitung (Art. 32)
Verarbeitungs-verzeichnis (Art. 30)	DS-Verletzung (Art. 33,34)	Folgenabschätzung (Art. 35,36)
DSB (Art. 37-39)		

3	Wahrung der Betroffenenrechte sicherstellen	
Information (Art. 13,14)	Auskunftsrecht (Art. 15)	Berichtigung (Art. 16,19)
Löschung (Art. 17,19)	Beschränkung (Art. 18,19)	Übertragbarkeit (Art. 20)
Widerspruch (Art. 21)	Automatisierte Entscheidung (Art. 22)	DS-Verletzung (Art. 34)
Widerruf (Art. 7)		

1) Technische und organisatorische Maßnahmen

Quelle: Ritterwald

Das Verständnis der DSGVO ermöglicht wesentliche Datenschutzprozesse zu identifizieren

Datenschutzrechtliche Kernprozesse

Datenschutzkonforme Datenverarbeitung

Sicherstellung der Betroffenenrechte

Handhabung von Datenschutzverletzungen

Quelle: Ritterwald / Kranig, Sachs, Gierschmann

Neben den Datenschutzprozessen bedarf es bestimmter organisatorischer Strukturen

Wesentliche Datenschutzstrukturen (Aufbauorganisation)

Datenschutzziele

- Leiten sich aus dem Sinngehalt der DSGVO sowie aus internen Anforderungen
- Müssen durch die Geschäftsleitung als Unternehmensziele benannt werden

Datenschutz-Governance-Struktur

- Definition von Rollen und Verantwortlichkeiten

Datenschutzleitlinie

- **Fasst die definierten Ziele sowie Rollen und Verbindlichkeiten in Form einer Selbstverpflichtung zusammen**
- Manifestierte das strategische Rahmengerüst wie Datenschutz-Compliance im Unternehmen erreicht werden soll, z.B. durch Einführung eines Data Protection Management System (DPMS)
- Beinhaltet keine Schritt für Schritt Anleitung, diese ist Teil des Datenschutz-Handbuchs

Quelle: Ritterwald

Unternehmen müssen überprüfen, ob die Verarbeitung mit der DSGVO konform ist

Datenschutzkonforme Datenverarbeitung

Verantwortliche müssen den rechtmäßigen Umgang mit Daten nachweisen (Art. 5)

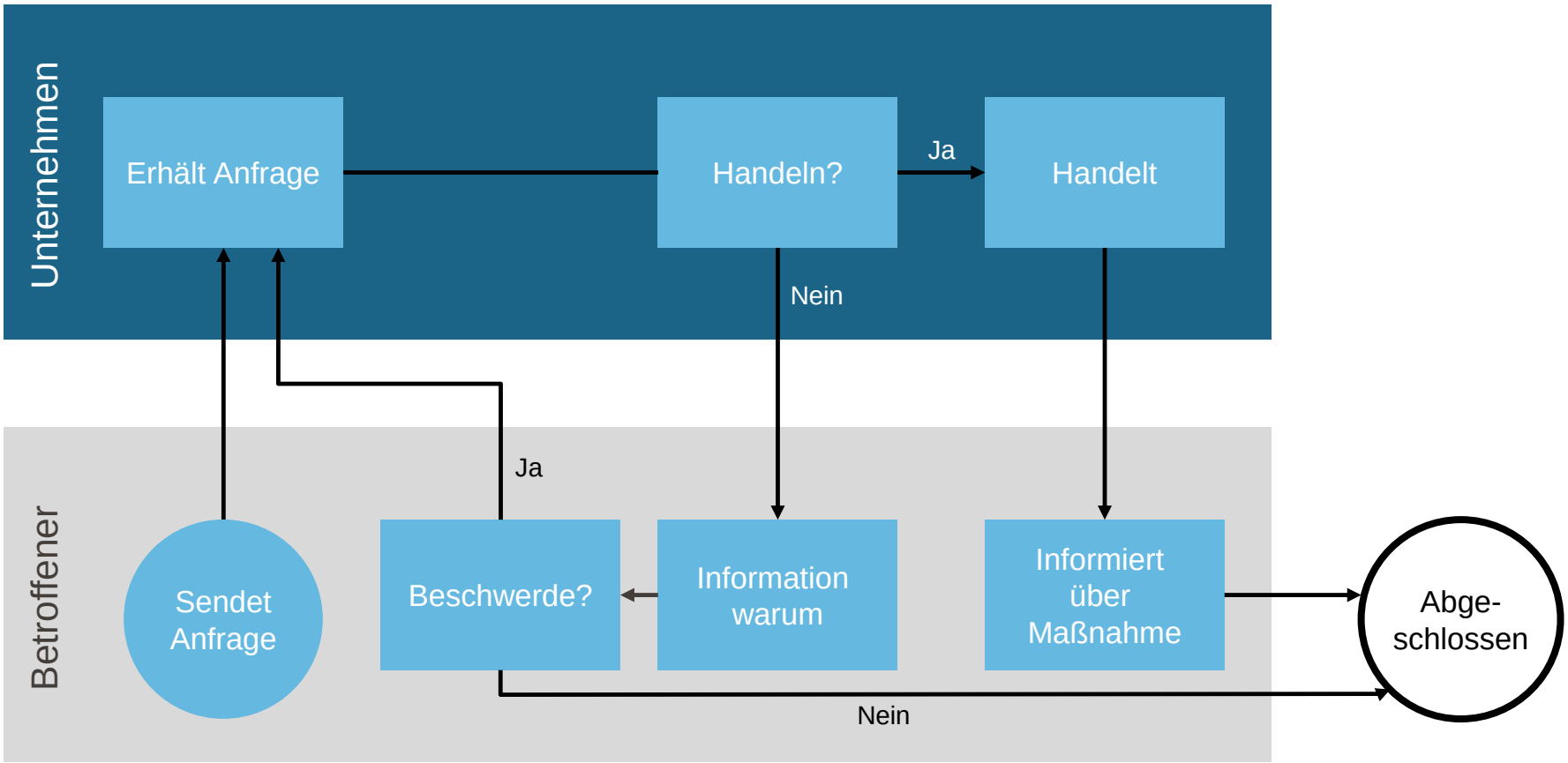
Verarbeitung personenbezogener Daten

Recht-mäßigkeit (Art. 6)	Transparenz (Art. 12)	TOM (Art. 24)	Auftrags-verarbeitung (Art. 28)	Sicherheit (Art. 32)	Verzeichnis (Art. 30)	Übertragung (Art. 44)

Quelle: Ritterwald

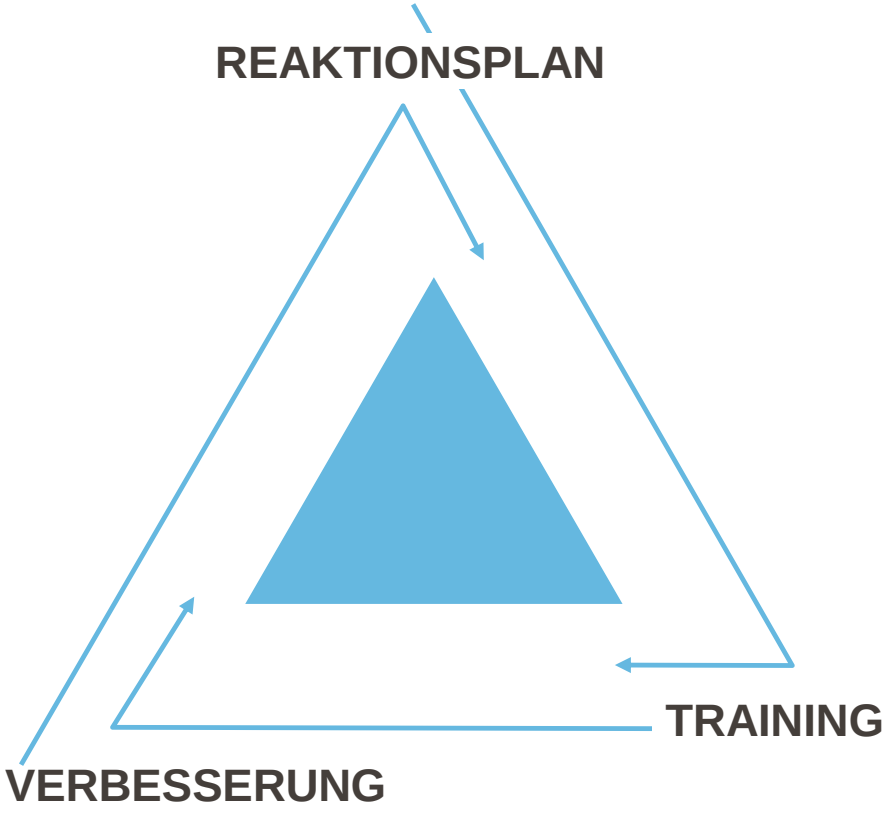
Unternehmen müssen Prozesse schaffen, um Anfragen von Betroffenen in Übereinstimmung mit der DSGVO zu verarbeiten

Sicherstellung der Betroffenenrechte



Unternehmen sollten auf Datenschutzverletzungen vorbereitet sein und einen Plan für Datenschutzverletzungen vorhalten

Handhabung von Datenschutzverletzungen



REAKTIONSPLAN ELEMENTE

- **Identifikation von Datenschutz-verletzungen**
  - **Risikoanalyse**
    - Welche Art von Verletzung?
    - Welche Art von Daten?
  - **Auswahl von Maßnahmen**
    - Was sind angemessene Maßnahmen?
    - Können wie sie sofort umsetzen?
  - **Entscheidung über Benachrichtigung**
    - Sind wir verpflichtet, die Aufsichtsbehörden oder die Betroffenen zu informieren?
  - **Durchführung der Benachrichtigung**

Quelle: Ritterwald

Kontakt

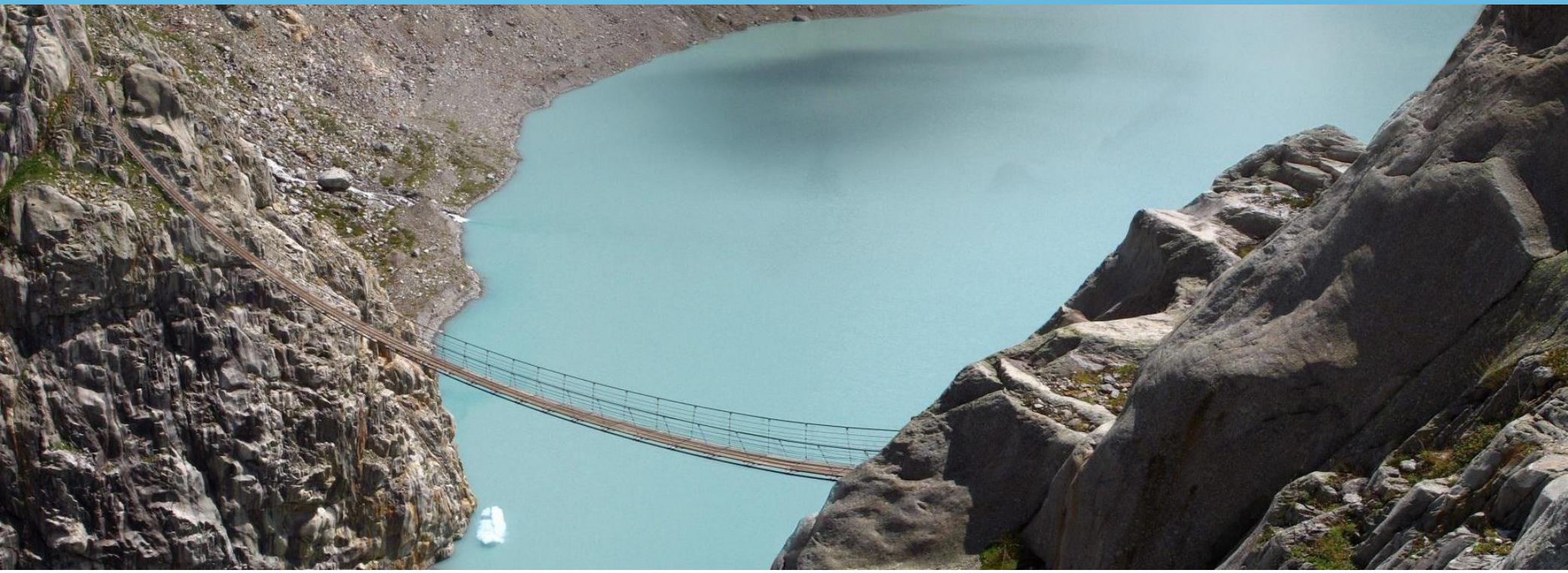
PARTNER
Ritterwald Unternehmensberatung GmbH
Kurfürstendamm 22 (Kranzler Eck Berlin)
10719 Berlin

Telefon: +49 30 609 85 82 41
Fax: +49 30 609 85 82 42
Mobil: +49 173 90 15 111
E-mail: mathias.hain@ritterwald.de
www.ritterwald.de

PROJECT MANAGER
Ritterwald Unternehmensberatung GmbH
Kurfürstendamm 22 (Kranzler Eck Berlin)
10719 Berlin

Telefon: +49 30 609 85 82 40
Fax: +49 30 609 85 82 49
Mobil: +49 172 279 28 91
E-mail: holger.grueneberg@ritterwald.de
www.ritterwald.de

Wir beraten Unternehmen.
Mit Sorgfalt und Weitblick.



RITTERWALD

Unternehmensberatung

Disclaimer

Dieses Dokument wurde zur ausschließlichen Nutzung für unseren Klienten erstellt. Es ist ohne die zu Grunde liegenden Detailanalysen und den mündlichen Vortrag nicht vollständig. Eine Weitergabe an Dritte ist nur mit dem ausdrücklichen schriftlichen Einverständnis der Ritterwald Unternehmensberatung GmbH gestattet.

Dieses Dokument erhebt keinen Anspruch auf Vollständigkeit der für die Entscheidungsfindung des Adressaten benötigten Informationen. Es werden keine Garantien oder Zusicherungen, explizit oder implizit, für die Vollständigkeit oder Richtigkeit dieses Dokumentes oder sonstiger mündlicher oder schriftlicher Angaben im Verlauf des Projektes gegeben.

Ritterwald Unternehmensberatung GmbH schließt ausdrücklich jegliche Haftung für die in diesem Dokument enthaltenen, möglicherweise fehlerhaften sowie gegebenenfalls ausgelassenen Informationen aus. Im Besonderen wird keine Garantie für die Erreichung oder Plausibilität der beschriebenen Zukunftsprognosen, Geschäftsführungsziele oder wirtschaftlichen Aussichten gegeben.