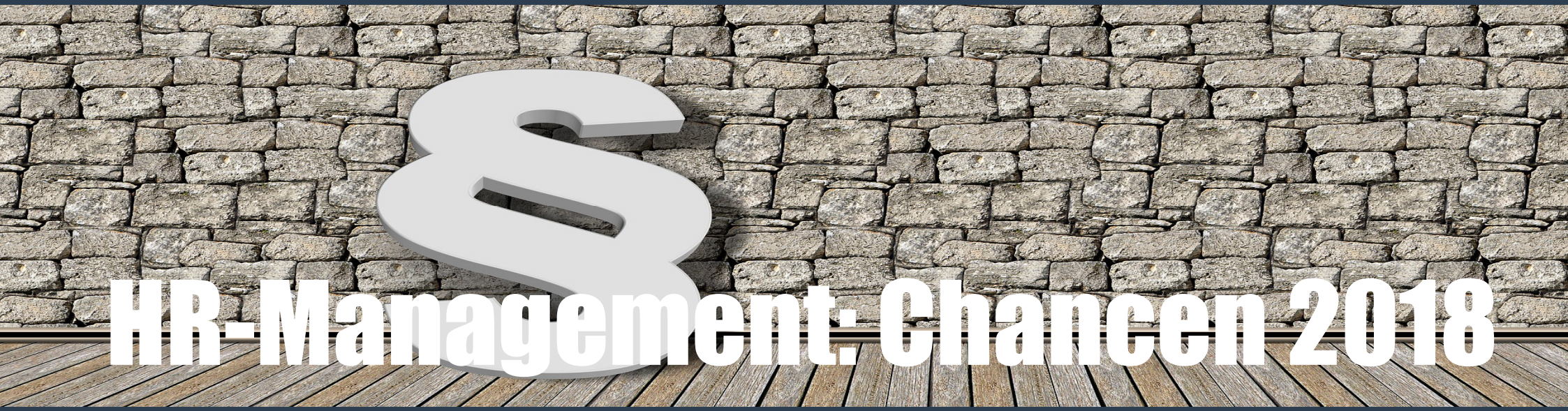


# HR-Management: Chancen 2018

EU-DSGVO und die Notwendigkeit transparenter HR-Prozesse

HR II
UNTERNEHMENSBERATUNG

# EU-Datenschutzgrundverordnung zum 25. Mai 2018

## Die EU-Datenschutzgrundverordnung (DS-GVO) tritt Ende Mai 2018 in Kraft. HR-Bereiche müssen sich bis dahin wappnen, um potenziellen empfindlichen Strafen zu entgehen.

Alle Unternehmen, die personenbezogene Daten erheben, verarbeiten, nutzen und speichern, haben noch bis Mai 2018 Zeit, ihre Datenverarbeitungsprozesse an die neuen gesetzlichen Rahmenbedingungen anzupassen. Aufgrund der vielen neuen Regelungen und Anforderungen sowie der stark erhöhten Bußgeldandrohungen (bis zu 20 Mill. €) müssen Unternehmen schnellstens beginnen, sich mit den kommenden Veränderungen im Umgang mit personenbezogenen Daten vertraut zu machen, um die Übergangszeit konstruktiv zu nutzen.

Darüber hinaus ist Datenschutz nicht länger nur eine Option, sondern vielmehr ein Muss. Denn Versäumnisse in diesem Bereich können sich nicht nur in finanzieller Hinsicht negativ auf ein Unternehmen auswirken, sondern auch das Vertrauen von Bewerbern, Kunden, Partnern, Dienstleistern und ehemaligen Mitarbeitern (Alumni) nachhaltig erschüttern. Ein angemessenes und umgesetztes Datenschutzsystem ist somit ein sehr guter Schutz für das Unternehmen, um folgende Risiken zu minimieren bzw. auszuschließen.

- Hohe Bußgelddrohungen
- Rufschädigung / Reputationsverlust
- Schadensersatzpflicht gegenüber Dritten

Die EU-Datenschutz-Grundverordnung verpflichtet Verantwortliche gewisse, allgemeine Grundsätze bei der Verarbeitung personenbezogener Daten einzuhalten. Zudem muss dies dokumentiert werden. Die Grundsätze stellen die Spielregeln dar, welche bei jeglicher Verarbeitung von personenbezogenen Daten zu beachten sind.

# DS-GVO – Um welche Daten geht es genau?

## HR hat verarbeitet im Rahmen der typischen Aufgaben grundsätzlich personenbezogene und damit sensible und besonders schützenswerte Daten.

**Auszug aus dem Bundesdatenschutzgesetz (BDSG)**

§ 3 Absatz 1 BDSG

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

§ 3 Absatz 9 BDSG

Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Auszug aus einer Kommentierung: Personenbezogene Daten

Nach § 3 Absatz 1 BDSG handelt es sich dabei um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Damit sind also alle Informationen umfasst, die etwas über den Betroffenen aussagen können.

Das Bundesdatenschutzgesetz enthält insbesondere in den §§ 13 Absatz 2, 28 Absatz 6 bis 9 und 29 Absatz 5 BDSG Sonderregelungen für die besonderen Arten personenbezogener Daten. § 3 Absatz 9 BDSG regelt abschließend, um welche Daten es sich dabei handelt (vgl. oben). Es handelt sich insoweit also um besonders sensible Daten.

Bei der Implementierung der meisten HR-Systeme in Unternehmen lag der Fokus auf der Abbildung von HR-Prozessen. In dieser Zeit waren die Anforderungen an den Datenschutz noch nicht so strikt geregelt wie mittlerweile. Die gesetzlichen Vorgaben haben sich in den letzten Jahren stark verändert und verschärft – teilweise dem gesellschaftlichen Fokus hinsichtlich des Umgangs mit persönlichen Daten geschuldet.

# Die DS-GVO-Anforderungen umfassen 7 Rubriken

## HR ist v.a. bei 3 Anforderungsrubriken stark in der Verantwortung für das gesamte Unternehmen

**Die Anforderungen der DS-GVO lassen sich in insgesamt 7 Rubriken einteilen.**

- Datenerhebung- und Verarbeitung
- Informationspflichten
- Betroffenenrechte
- Beziehungen zu Dienstleistern
- Sicherheitsmanagement
- Meldepflicht bei Verstößen
- Haftung und Bußgelder

HR ist v.a. bei den ersten 3 Rubriken stark verantwortlich; die letzten 4 sind v.a. auch im Verantwortungsbereich des Unternehmens / des Datenschützers allgemein.

Datenerhebung- und Verarbeitung: Gem. den Anforderungen der DS-GVO müssen personenbezogene Daten, deren Zweckbindung entfallen ist und keine gesetzlichen und betrieblichen Fristen zur Aufbewahrung entgegen stehen, vernichtet werden

Die Informationspflicht der verarbeitenden Stelle soll gegenüber dem Betroffenen sicherstellen, dass er zu jeder Zeit Kenntnis über den Verbleib seiner personenbezogenen Daten hat. Um der Informationspflicht nachzukommen, helfen die folgenden W-Fragen: Durch wen werden wo welche Daten wie lange gespeichert und was passiert mit Ihnen nach Ablauf der Zweckbindung.

Bei den Betroffenenrechten handelt es sich im Wesentlichen um das Recht auf Auskunft, Berichtigung, Löschung sowie Einschränkung der Verarbeitung von personenbezogenen Daten. Das Recht auf Berichtigung muss oftmals nicht betrachtet werden, da fehlerhafte personenbezogene Daten, deren Verarbeitung erforderlich ist, i.d.R. immer berichtigt werden

# Die DS-GVO verschärft die Regelungen des BDSG weiter

Die Anforderungen an HR nehmen v.a. bezüglich der Betroffenenrechte zu, da die DS-GVO einen noch besseren Schutz von personenbezogenen Daten bieten soll als das BDSG.

| Ausgewählte Rechte von Betroffenen | DS-GVO |
|---|---|
| Informationsrecht | Proaktive Benachrichtigung u.a. über Verarbeitungszwecke von Daten, Rechtsgrundlage, Dauer der Speicherung |
| Auskunftsrecht | Verlangen einer Bestätigung über die Verarbeitung von personenbezogenen Daten |
| Berichtigungsrecht | Verlangen der Berichtigung unzutreffender personenbezogener Daten |
| Löschungsrecht | Verlangen des Löschens von Daten unter Berücksichtigung bestimmter Ausnahmen (z.B. Daten sind zu ursprünglichem Erhebungszweck nicht mehr erforderlich) |
| Einschränkung der Verarbeitung | Verlangen der Einschränkung der Verarbeitung von betreffenden personenbezogenen Daten z.B. für die Dauer einer möglichen Richtigkeitsüberprüfung durch den Betroffenen |
| Recht auf Datenübertragbarkeit | Neueinführung des Rechts auf Datenübertragbarkeit mit dem Anspruch, unter bestimmten Voraussetzungen eine Kopie der sie betreffenden personenbezogenen Daten zu erhalten |

# Die neuen Regelungen betreffen v.a. die HR-Kernprozesse

## HR hat im Unternehmen bezüglich der DS-GVO zu Mai 2018 den höchsten Handlungsbedarf

| Ausgewählte HR-Kernprozesse | Beispiele zur Datenverarbeitung personenbezogener Daten |
|---|---|
| Recruiting | • Eingabe und Speicherung von Bewerberdaten wie Name, Adresse, Bankdaten zur Erstattung von Vorstellkosten, Zeugnisse und sonstige Unterlagen in Bewerbermanagement-Systemen |
| Einstellung | • Verarbeitung von Mitarbeiterdaten wie Name, Adresse, Zeugnisse und sonstige Unterlagen, Anlage Personalnummer, Gehaltsdaten, vorherige Beschäftigungen in Systemen, Dateien und Personalakte |
| Personalbetreuung | • Verarbeitung von Mitarbeiterdaten wie Beurteilungsbögen, Mitarbeitergespräche, Zielvereinbarungen, Versetzungen / Umsetzungen, Gehälter, Leistungsprämien, Gehaltsentwicklung in Systemen, Dateien und Personalakte |
| Gesundheits-Management | • Verarbeitung von Gesundheitsspezifischen Daten zum Mitarbeiter sowie präventive Maßnahmen in Systemen und Dateien |
| Alumni-Betreuung | • Speichern von Alumni-Daten wie Name, Adresse, Grades, …in Systemen und Dateien |

# HR muss die Umsetzung der DS-GVO vorantreiben

HR muss die Umsetzung der sich aus der DS-GVO abzuleitenden Anforderungen von personalwirtschaftlichen Daten sicherstellen.

Dr. Heiko Lorson

h.lorson@hrzwei.de

**1** Bedarfsanalyse HR auf Basis DS-GVO (Prozesse, Systeme)

**2** HR-Prozessbe-schreibung/-ergänzung inkl. Speicherorte / IT-Systeme

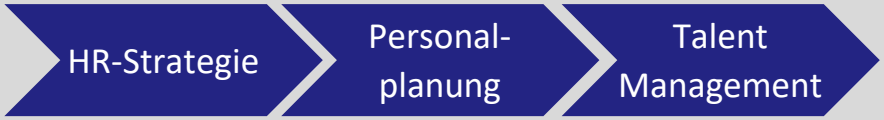
**3** Technische Umsetzung der DS-GVO-Anforderungen in HR-IT

4 Definition HR-Datenlöschen-Prozess

# 1. Bedarfsanalyse eines möglichen Handlungsbedarfs

In einem ersten Schritt muss zunächst festgestellt werden, welchen Handlungsbedarf vor dem Hintergrund der EU-Datenschutzgrundverordnung HR hat.

**HR-Managementprozesse**




**HR-Kernprozesse**

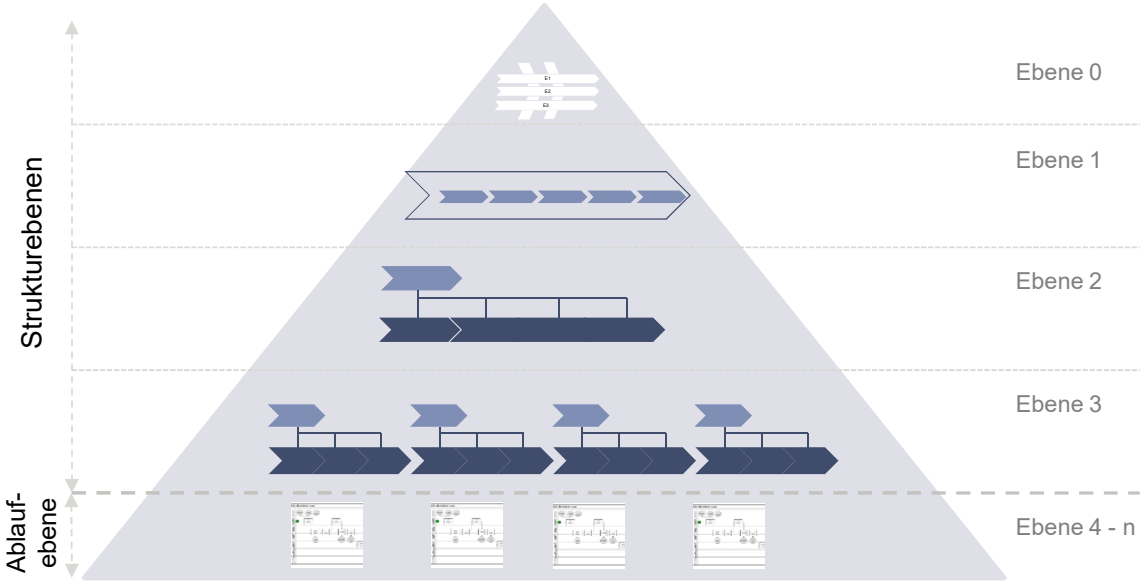
**HR-Unterstützungsprozesse**

Hier muss HR u.a. folgende Fragen beantworten:

- Welche HR-Prozesse sind konkret betroffen von der DS-GVO? (z.B. Recruiting, Betreuung, Reporting, Gesundheitsmanagement, …)
- Kann HR Auskunft darüber geben in welchem HR-Prozess in welchem System / in welchem SAP-Infotyp welche Daten abgelegt / gespeichert / gelöscht werden?
- Sind die betroffenen HR-Prozesse dokumentiert, auch für Dritte?
- …

# 2. Aufnahme und Ergänzung von HR-Prozessen (1/2)

In einem zweiten Schritt müssen die einzelnen HR-Prozess-Schritte transparent gemacht werden. Hierbei ist die einheitliche Strukturierung von Prozessen ein wirksames Mittel.



Heiko Lämmrich

h.laemmrich@hrzwei.de

Aus Unternehmenssicht sind auf Ebene 0 alle Hauptprozesse festgelegt, die alle Aktivitäten im Unternehmen beschreiben. Eine detailliertere Prozess-Beschreibung folgt entsprechend auf den weiteren Ebenen.

# 2. Aufnahme und Ergänzung von HR-Prozessen (2/2)

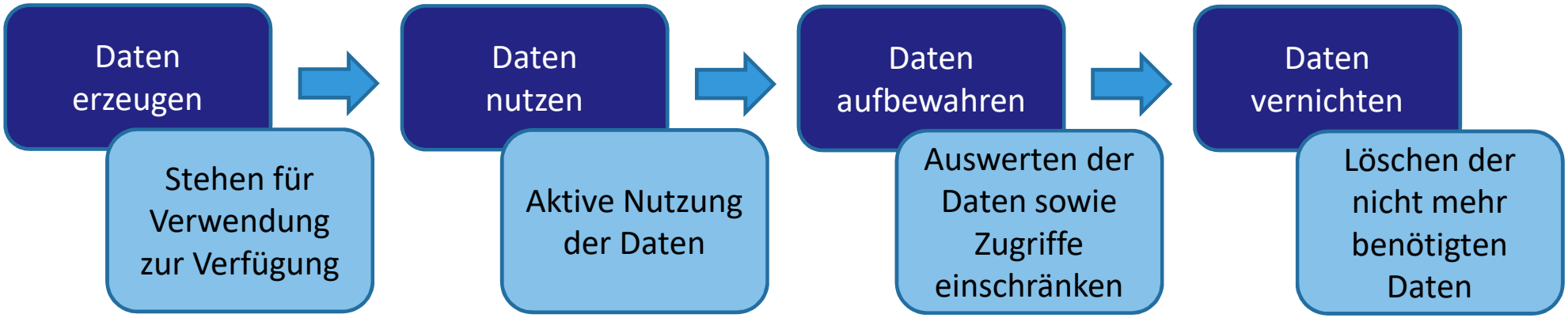
Im zweiten Schritt muss auch aufgezeigt werden, in welchen Systemen personenbezogene Daten verarbeitet werden.

| Prozessebene 1 | Prozessebene 2 | Prozessebene 3 | Verantwortung | Speicherort |
|---|---|---|---|---|
| Recruiting | Stellenanforderung erstellen und veröffentlichen | Stellenanforderung / Ausschreibung erstellen | Referent | Bewerbermanagement-System, Lokale Datenablage |
| | | Interne Stellenausschreibung durchführen | | |
| | | Externe Stellenausschreibung durchführen | | |
| | | Headhunter briefen und beauftragen | | |
| | Bewerbungen sichten und bewerten | Bewerbungen sichten | | |
| | | Vorauswahl treffen | | |
| | | Absagen versenden | | |
| | | Einladungen zu Telefoninterview versenden | | |
| | Bewerber auswählen und entscheiden | Telefoninterview durchführen (ca. 30 min) | Fachbereich | |
| | | Absagen versenden | Referent | |
| | | Einladungen zu Vorstellungsgespräch versenden | Referent | |
| | | Vorstellungsgespräch durchführen | Referent / Fachbereich | |
| | | Entscheidung bezüglich Bewerber fällen | Referent / Fachbereich | |
| | | Absagen versenden | Referent | |
| | | Zusagen mitteilen | Referent | |
| | | Onboarding einleiten | Referent | |

# 3. Technische Umsetzung in HR-IT-Systemen

In einem dritten Schritt muss die DS-GVO in den HR-IT-Systemen gemäß den definierten Anforderungen umgesetzt werden inklusive der Festlegung von Datenlöschfristen.

**Recht** **auf:** **Auskunft Information** **„Vergessen werden“**



# 4. Definition eines Regelprozesses „HR-Daten löschen“

## Es muss letztlich neben den HR-Management-, Kern- und Unterstützungsprozessen grundsätzlich ein HR-Datenlöschprozess definiert werden.

Da gemäß der DS-GVO Artikel 5 die Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, müssen für die Verarbeitung bestimmte Bedingungen erfüllt werden. Im Wesentlichen handelt es sich um

- die Rechtmäßigkeit,
- die Verarbeitung nach Treu und Glauben sowie
- die Transparenz

Weiterhin müssen die Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Erhebung muss dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Weitere Grundsätze sind dem Test der Verordnung, Artikel 5, zu entnehmen. Vor diesem Hintergrund müssen Unternehmen die bereits bzw. zukünftig erhobenen Daten in Bezug auf die Rechtmäßigkeit und Zweckbindung identifizieren, klassifizieren sowie den Umgang mit den Daten festlegen.

Die DS-GVO sieht eine Löschpflicht vor, sobald die Zweck-bindung der Daten entfallen ist und keine gesetzlichen Aufbewahrungsfristen entgegen stehen. Die DS-GVO sieht keine Regelungen vor, die sich auf die Daten an sich festlegen. Es ist also nicht möglich, sich auf die Verordnung zu berufen und die Personalbestandsdaten vollständig bis zum Ablauf der längsten Aufbewahrungsfrist in den HR IT-Systemen zu behalten. Vielmehr müssen die Daten aus den HR IT-Systemen gelöscht werden, sobald deren zugeordnete Aufbewahrungsfrist abgelaufen ist. Ist die längste Aufbewahrungsfrist abgelaufen, ist auch die Person als solches aus den HR IT-Systemen zu löschen. Im Ergebnis ist die Person nicht mehr in den HR IT-Systemen vorhanden. Das Recht auf „vergessen werden“ ist dann vollständig umgesetzt.

# IMPRESSUM

**Ort und Datum der Veröffentlichung**

München 02/2018

Diese Veröffentlichung wurde in Zusammenarbeit zwischen
HR II Unternehmensberatung und Baumgartner & Partner erstellt.

**Autoren**

Dr. Heiko Lorson
Heiko Lämmrich

**Herausgeber**

Baumgartner & Partner
Management Consultants GmbH
Straßenbahnring 17

20251 Hamburg
Germany
www.baumgartner.de

**Kontakt**
ralf.kleb@baumgartner.de

HR II Unternehmensberatung

Seybothstraße 7

81545 München
Germany
www.hrzwei.de

**Kontakt**
h.lorson@hrzwei.de

**Disclaimer**

These publications are provided for general information purposes only. Your use of any of these whitepapers is at your own risk, and you should not use any of these documents without first seeking professional and/or legal advice. The provision of these documents (and the documents themselves) do not constitute legal advice or opinions of any kind, or any advertising or solicitation. No lawyer-client, advisory, fiduciary or other relationship is created between Baumgartner & Partner Management Consultants GmbH, HR II Unternehmensberatung and any person accessing or otherwise using any of the documents. Baumgartner & Partner Management Consultants GmbH and HR II Unternehmensberatung (and any of their respective directors, officers, agents, contractors, interns, suppliers and employees) will not be liable for any damages, losses or causes of action of any nature arising from any use of any of the documents or the provision of these documents.

© HR II Unternehmensberatung und Baumgartner & Partner 2018