



Sensible Unternehmensdaten Kivitendo und Datenschutz

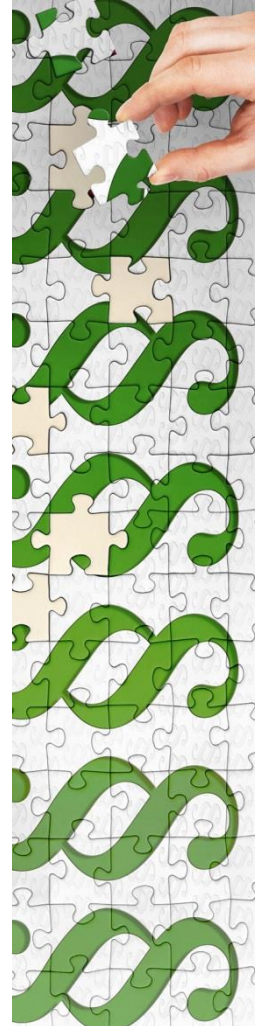
28.04.2016
Claus Wissing
WiR Solutions GmbH

Externer Datenschutzbeauftragter und
Sachverständiger für IT-Sicherheit



Agenda

- ✓ Wer ist die WiR Solutions GmbH
- ✓ Was bedeutet Datenschutz? Das Bundesdatenschutzgesetz (BDSG)
- ✓ Aspekte des Datenschutzes bei kivitendo
- ✓ Praktizierter Datenschutz im Büroalltag



Wer sind WiR?

- ✓ Die WiR Solutions GmbH ist ein unabhängiges Unternehmen aus dem Münsterland und in ganz Deutschland tätig
- ✓ Dipl.-Ingenieure mit langjähriger Erfahrung in der Telekommunikations-, IT- und Informatik-Branche
- ✓ Kernbereiche: IT- und IT-Sicherheitsprojekte, Breitbandprojekte, Datenschutz incl. Bereitstellung externer Datenschutzbeauftragter
- ✓ Die WiR ist seit 2006 stetig wachsend am Markt und hat 28 Experten
- ✓ Know-How gepaart mit ergebnisorientiertem und pragmatischem Vorgehen
- ✓ Zusammenarbeit mit Partnern für flexible und für den Kunden passende Lösungen
 - ✓ WiR schaffen Lösungen
 - ✓ WiR senken Kosten
 - ✓ WiR dienen dem Kunden.



FAM²TEC
Mehr Frauen in MINT



Leitsätze des Datenschutzes

- ✓ Die Daten unserer Mitarbeiter, Kunden und Partner sind uns sehr wichtig und sollen mit der notwendigen Sorgfalt behandelt werden!
- ✓ Behandeln Sie die Daten anderer so, wie Sie selbst Ihre eigenen Daten behandelt wissen möchten!
- ✓ Datenschutz bedeutet schlichtweg vernünftiger und verantwortungsvoller Umgang mit jeglichen Daten im Unternehmen!

Einführung in den Datenschutz

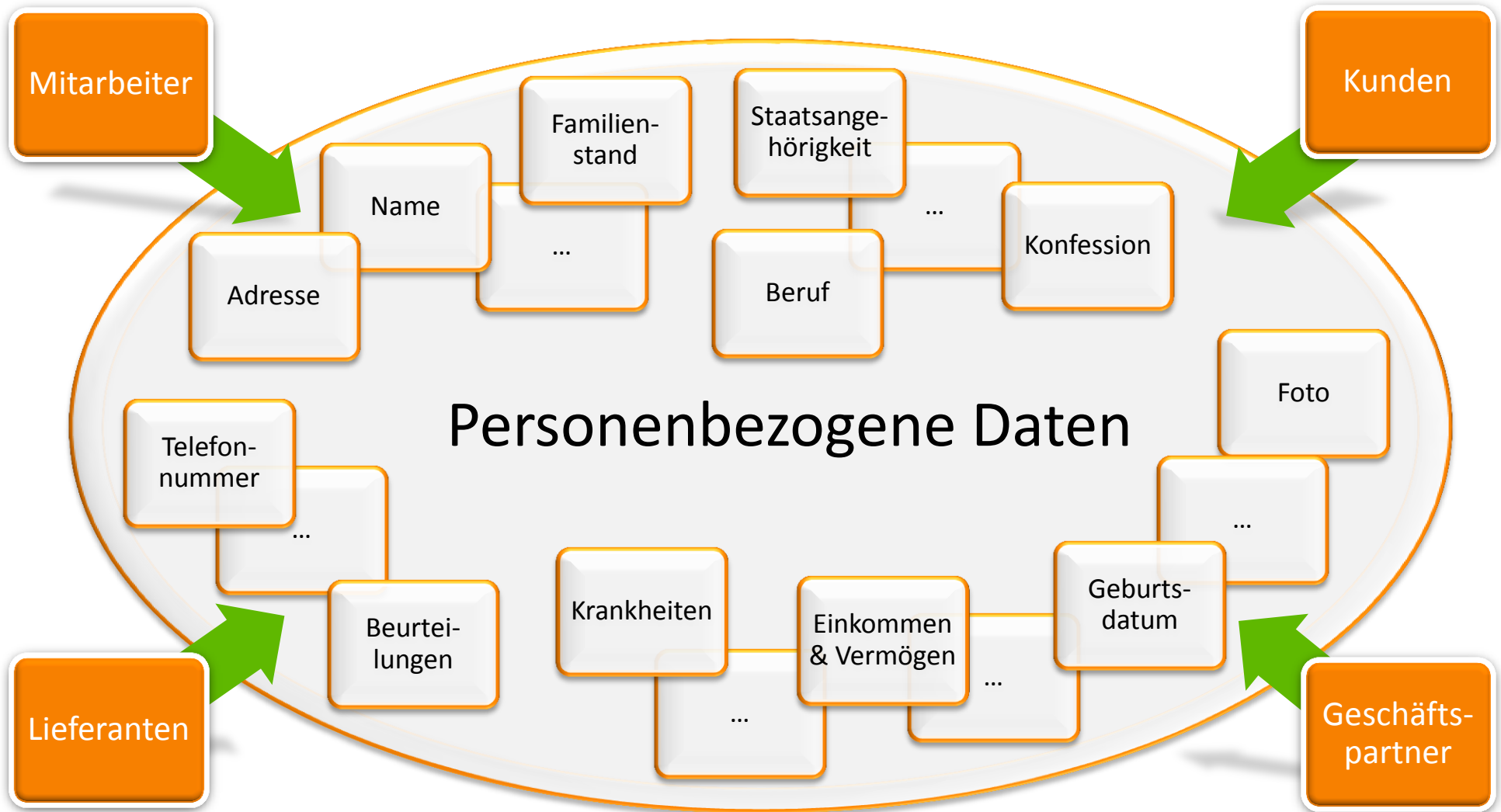
Was ist Datenschutz?

- ✓ Personen sollen vor unbefugter Verwendung oder Weitergabe ihrer persönlichen Daten geschützt werden!
- ✓ Der Datenschutz ist abgeleitet aus den Artikeln 1 und 2 des Grundgesetzes:
 - Die Würde des Menschen ist unantastbar (Art. 1, Abs. 1, S. 1 GG).
 - Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit [...] (Art. 2 GG).
- ✓ Schutz des Rechts auf informationelle Selbstbestimmung (BVerfG-Urteil)

Gegenstand des Datenschutzes sind personenbezogene (und personenbeziehbare) Daten. Datenschutz hat den Schutz der Privatsphäre des Einzelnen zum Ziel!



Das Bundesdatenschutzgesetz (BDSG)



Besonders sensible Daten laut Bundesdatenschutzgesetz (BDSG)



Das Bundesdatenschutzgesetz (BDSG)

Grundsätzliches zum Bundesdatenschutzgesetz

- ✓ Das Bundesdatenschutzgesetz (BDSG) regelt den Umgang mit "personenbezogenen Daten" in Deutschland und ist die gesetzliche Grundlage für den Datenschutz.
- ✓ Das BDSG ist für alle so genannten "nicht-öffentlichen Stellen", also die Unternehmen in Deutschland und für alle Bundesbehörden bindend (ausgenommen sind rein private oder familiäre Zweckbestimmungen).
- ✓ Verantwortlich ist zwar die jeweilige Geschäftsführung, allerdings hat auch jeder Mitarbeiter das Gesetz zu beachten.

Die Vorgaben des Bundesdatenschutzgesetzes gelten für alle Unternehmen – unabhängig von Größe, Tätigkeit oder Pflicht zur Bestellung eines Datenschutzbeauftragten!



Das Bundesdatenschutzgesetz (BDSG)

Die Grundsätze der Datenerhebung, -verarbeitung und -nutzung im Sinne des Bundesdatenschutzgesetzes:

Datenvermeidung



Datensparsamkeit

„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“

(§3a, S. 1 BDSG)

Dies kann bei vertretbarem Aufwand auch eine Anonymisierung oder Pseudonymisierung der Daten bedeuten!



Das Bundesdatenschutzgesetz (BDSG)

Die Zweckbindung

- ✓ Der Umgang mit personenbezogenen Daten wird vom Zweck bestimmt:
 - Warum erheben wir diese Daten?
 - Werden alle Daten wirklich benötigt?
 - Ist der Zweck zulässig?

- ✓ Der so bewertete Zweck sollte die Erhebung, Verarbeitung und Nutzung im Sinne der Datenvermeidung und Datensparsamkeit auf das notwendige Maß beschränken.

Die Zweckbindung als zentrales Thema im BDSG ist zugleich die Begründung sowie die Beschränkung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten!



Das Bundesdatenschutzgesetz (BDSG)

Rechtliche Voraussetzungen

- ✓ Nach dem § 4 (1) BDSG dürfen personenbezogene Daten nur erhoben, verarbeitet oder genutzt werden, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder wenn der Betroffene eingewilligt hat.
- ✓ Also Erlaubnis der Datenerhebung, -verarbeitung und -nutzung durch:
 - Bundesdatenschutzgesetz (z.B. die Verarbeitung für eigene Geschäftszwecke, wenn eine vertragliche Grundlage vorliegt).
 - andere Rechtsvorschrift (z.B. Erhebung und Übermittlung von Arbeitnehmerdaten nach dem Sozialgesetzbüchern).
 - Einwilligung (z.B. freiwilliges Unterschreiben einer Einverständniserklärung zur Erhebung und Speicherung der angegebenen personenbezogenen Daten).

Das Bundesdatenschutzgesetz (BDSG)

Die Einwilligung

- ✓ Eine Einwilligung ist nur wirksam, wenn sie
 - **freiwillig** (ohne Druck oder begleitende Bedingungen) und
 - **ausreichend informiert** erteilt wird (derjenige, der seine Einwilligung gibt, hat ein Recht auf Information hinsichtlich der Datennutzung).
- ✓ Die Einwilligung
 - muss i.d.R. schriftlich sein,
 - darf nicht im „Kleingedruckten“ versteckt werden und ist optisch besonders hervorzuheben, wenn sie im Zusammenhang mit anderen Erklärungen steht.
 - muss besondere Arten von personenbezogenen Daten ausdrücklich erwähnen/aufführen.
- ✓ Die **elektronische Form der Einwilligung** (z.B. in der Internet-Kommunikation) ist grundsätzlich zulässig, unterliegt aber gewissen Vorgaben!
- ✓ Diese Einwilligung sollte nachvollziehbar dokumentiert werden.

Das Bundesdatenschutzgesetz (BDSG)

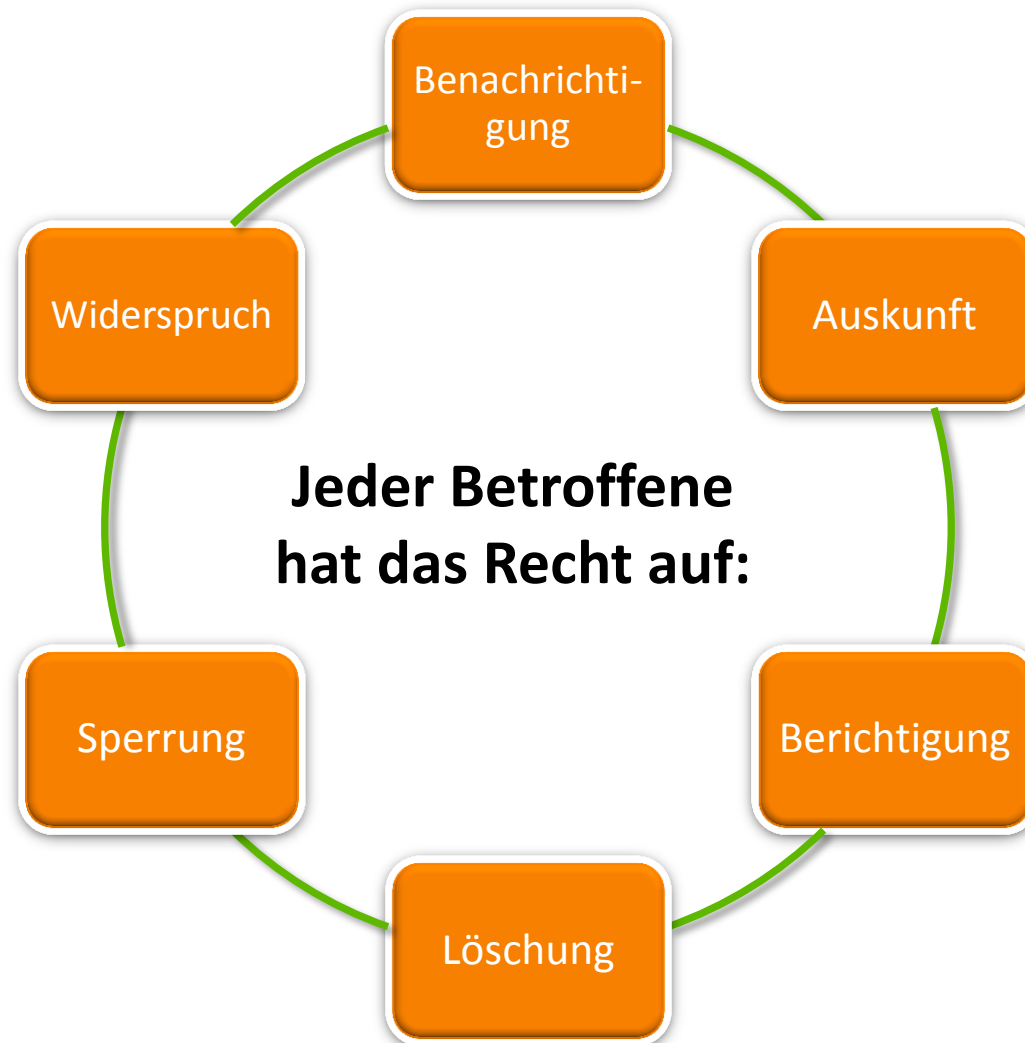
Der Datenschutzbeauftragte

- ✓ Innerhalb des Unternehmens hat z.B. der interne oder externe Datenschutzbeauftragte die Aufgabe, **auf die Einhaltung des BDSG hinzuwirken**.
- ✓ Unternehmen, die EDV-basiert in der Regel mit mehr als neun Mitarbeitern ständig personenbezogene Daten (also insbesondere Mitarbeiter- und Kundendaten) verarbeiten, benötigen gemäß § 4f BDSG einen internen oder externen Datenschutzbeauftragten.
- ✓ Nicht-öffentliche Stellen sind zur Bestellung eines Datenschutzbeauftragten spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet!

Der Datenschutzbeauftragte (DSB) kann ein interner oder externer Mitarbeiter sein! Auf jeden Fall sollte der DSB selbst und die Erreichbarkeit bekannt sein.



Der Betroffene



Datenschutz kontrollieren

Die Datenschutz-Aufsichtsbehörde

- ✓ ist eine Landesbehörde (und jeweils für die im Bundesland befindlichen Unternehmen und Landesbehörden zuständig),
- ✓ kontrolliert die Anwendung und Einhaltung der Datenschutzvorschriften,
- ✓ berät das Unternehmen und den Datenschutzbeauftragten auf Antrag,
- ✓ überprüft und sanktioniert Verstöße.

Die zuständige Aufsichtsbehörde darf ohne Begründung Kontrollen vornehmen!



Aspekte des Datenschutzes im Unternehmen

Das Datengeheimnis (§5 BDSG)

- ✓ Alle Mitarbeiter, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, haben Verschwiegenheit über die ihnen bekannt gewordenen Informationen zu wahren.
- ✓ Diese Mitarbeiter sind bei der Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis zu verpflichten und entsprechend über die besonderen Anforderungen des Datenschutzes zu unterrichten. Diese Schulung dient auch diesem Zweck

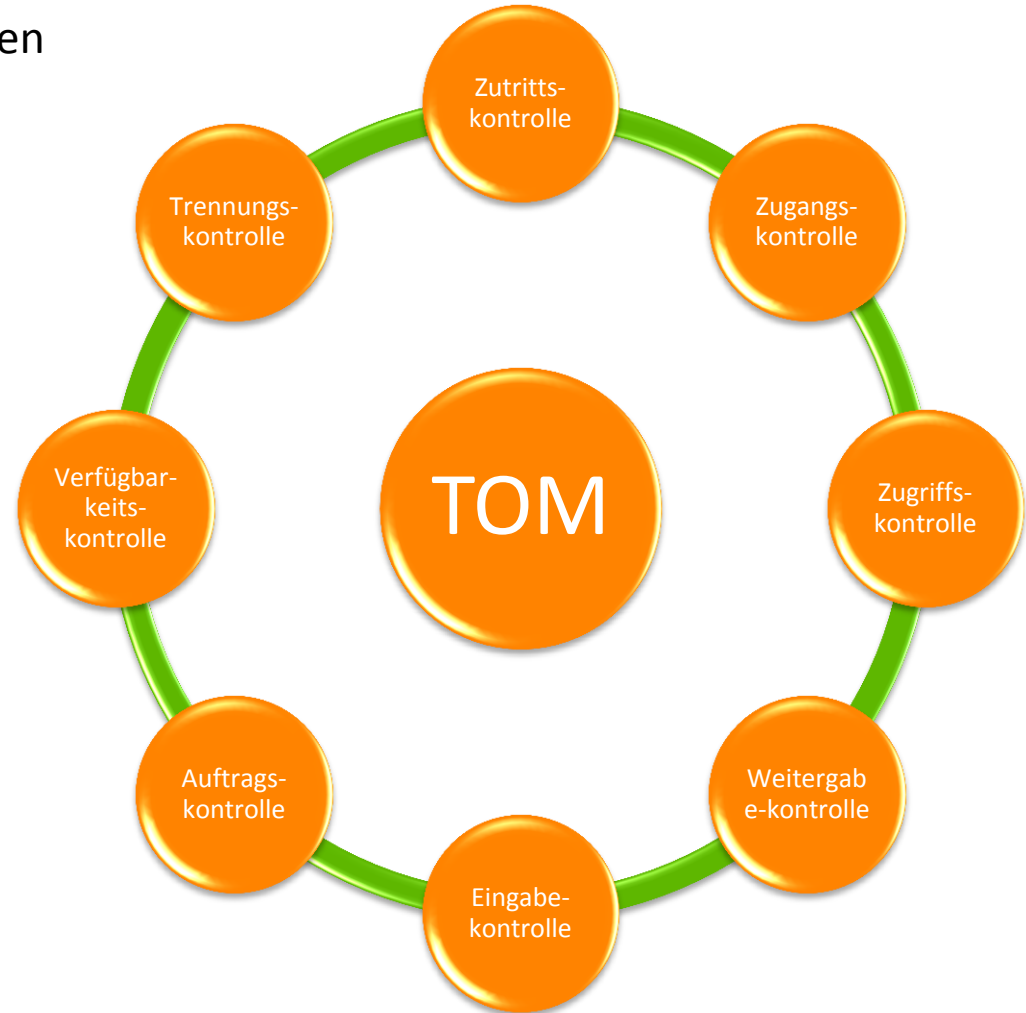
Das Datengeheimnis besteht auch nach Ende der Tätigkeit fort!



Aspekte des Datenschutzes im Unternehmen

Technische und organisatorische Maßnahmen (TOMs § 9 BDSG)

- ✓ Technische und organisatorische Maßnahmen sollen die Ausführung der Vorschriften des Bundesdatenschutzgesetzes und insbesondere die nebenstehenden Anforderungen (Anlage zu §9 Satz 1) sicherstellen.
- ✓ Der damit verbundene Aufwand muss dabei in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.



Aspekte des Datenschutzes im Unternehmen

Sanktionen (§§ 43 und 44 BDSG):

- ✓ Der Gesetzgeber hat bei bestimmten Vergehen, insbesondere bei Datenmissbrauch, zahlreiche Sanktionen – von Geldbußen bis Freiheitsentzug – vorgesehen.
- ✓ Verstöße gegen datenschutzrechtliche Vorschriften können erhebliche Auswirkungen auf das Image und die Vertrauenswürdigkeit Ihres Arbeitgeber- und Unternehmens haben.

Die Außenwirkung unzureichenden Datenschutzes oder gar öffentlich gewordener Verstöße ist nicht zu unterschätzen!



Aspekte des Datenschutzes bei kivitendo

Diverse Punkte gilt es abzuwägen:

Angemessenheit:

- ✓ die zu treffenden Maßnahmen an den zu schützenden Unternehmenswerten zu orientieren haben. Hierfür bietet sich zunächst die Durchführung einer **Schutzbedarfsanalyse** als Grundlage eines **Sicherheitskonzepts** an, um zu ermitteln, welcher Schutz für die Informationen und die eingesetzte [Informationstechnik](#) erforderlich sowie angemessen ist.
- ✓ Insbesondere Bankdaten und besondere Arten von Daten sind hier relevant!

Fehlverhalten kann mit einem Bußgeld bis zu 300.000 € geahndet werden!

Wird Ihnen ein solcher Vorgang bekannt, informieren Sie sofort die Geschäftsleitung und den Datenschutzbeauftragten.



Aspekte des Datenschutzes bei kivitendo

Berechtigungskonzept:

- ✓ **Ich sehe was, was du nicht siehst**
- ✓ Allgemein anerkannt ist, dass es Bereiche gibt, die tatsächlich nur bestimmte Personen bzw. Abteilungen einsehen können. Dazu gehören etwa die **Personalabteilung und die Administratoren. Beide Gruppen genießen allerdings so etwas wie ein Alleinstellungsmerkmal, da sie notwendigerweise alles sehen können müssen.** In diesem Fall geht das auch vollkommen in Ordnung. Nur sonst eben nicht.
- ✓ Denn schließlich findet sich immer ein Grund, warum jede Abteilung auf die Daten der anderen Abteilung zugreifen können muss. Von Vertretungsregeln über Wissensmanagement bis hin zu „das haben wir schon immer so gemacht“ – **es gibt keinen Grund den es nicht gibt.**

Schaffen Sie sich ein für Ihr Unternehmen passendes rollenbasiertes Berechtigungskonzept!



Aspekte des Datenschutzes in Bezug auf kivitendo

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§11 BDSG) – Auftragsdatenverarbeitung (ADV):

Wenn die Verarbeitung personenbezogener Daten **das wesentliche Element einer Aufgabenübertragung auf eine andere rechtliche Einheit** darstellt und / oder die datenverarbeitende Stelle eine **Hilfs- oder Unterstützungsfunktion** ausübt, wird in aller Regel eine Auftragsdatenverarbeitung vorliegen:

- ✓ Datenverarbeitung **durch** Fremdfirmen:
z.B. EDV-Dienstleistung durch fremdes Rechenzentrum, Mailingaktionen durch Lettershop (Direktmarketing), (Fern-)Wartung der EDV-Systeme...
- ✓ Datenverarbeitung **für** Fremdfirmen (auch im Konzern!)
z.B. zentrale Bereitstellung von IT, zentrale Personalabteilung, Lohnabrechnung für Unternehmen im Konzern...

Die Verantwortung für die Einhaltung der Vorschriften über den Datenschutz verbleibt beim Auftraggeber! Schalten Sie im Zweifel immer den Datenschutzbeauftragten ein!



Aspekte des Datenschutzes in Bezug auf kivitendo

Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§11 BDSG) – Auftragsdatenverarbeitung (ADV):

- ✓ Grundsätze:
 - Der Auftragnehmer ist **sorgfältig** auszuwählen.
 - Der Auftrag ist **schriftlich** zu erteilen, und der Vertrag muss gemäß § 11 BDSG bestimmte Aspekte enthalten.
 - Vor Abschluss des Vertrags muss sich der Auftraggeber von der Einhaltung der getroffenen Sicherheitsmaßnahmen überzeugen.
 - Weitere **Kontrollen** können vereinbart werden.
- ✓ Benutzen Sie für die Vertragsgestaltung die in Ihrem Hause dafür vorgesehenen Musterklauseln bzw. schalten Sie Ihren Datenschutzbeauftragten ein.

Ein nicht richtig abgeschlossener Vertrag nach § 11 BDSG und die nicht durchgeführte Kontrolle des Auftragnehmers vor Beginn der Verarbeitung sind bußgeldbewehrt.



Praktizierter Datenschutz im Büroalltag

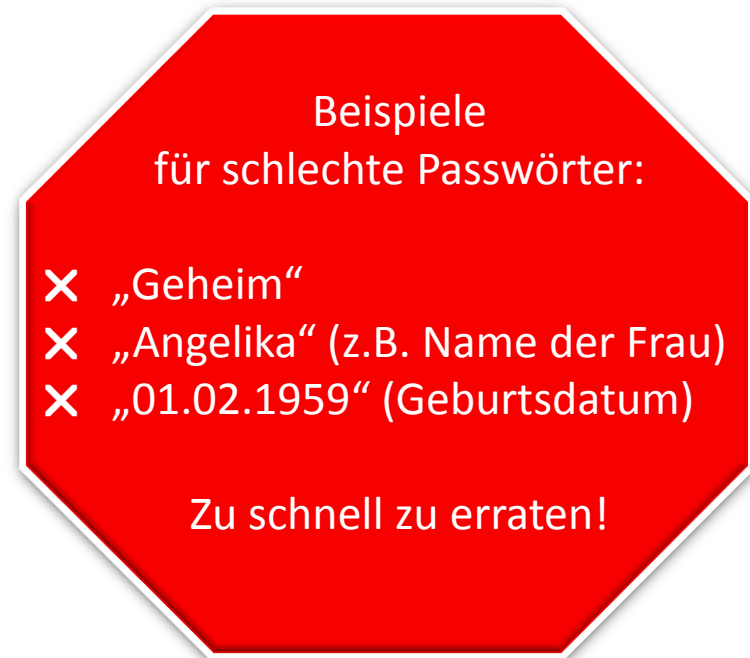
Nutzung von sicheren Passwörtern

Grundsätze für ein sicheres Passwort:

- ✓ mindestens 8 Zeichen
- ✓ Groß und Kleinschreibung verwenden
- ✓ Ziffern verwenden
- ✓ Sonderzeichen verwenden
- ✓ Regelmäßig ändern
- ✓ Sinnfreie Zusammensetzung

Ein gutes Passwort, z.B. ermittelt aus Sätzen, die nur Sie kennen:

- ✓ Sia31.D! Sylvester ist am 31. Dezember!
- ✓ lwadHs23a! Ich wohne an der Hansastr. 23a! (Bitte diese Beispiele nicht mehr als Passwörter verwenden)



Praktizierter Datenschutz im Büroalltag

E-Mail: praktisch, aber nicht ungefährlich!

- ✓ Vertrauliche Informationen grundsätzlich nicht über E-Mail versenden, wenn keine Verschlüsselung genutzt werden kann. Eine E-Mail ist vergleichbar mit einer Postkarte!
- ✓ Nicht einfach mit Antwortfunktion auf E-Mail reagieren, wenn Sie vertrauliche Inhalte einfügen. Vorher Absenderliste überprüfen!
- ✓ Keine Anlagen/Attachments von überraschenden/ ungewöhnlichen E-Mails öffnen, auch wenn der Absender bekannt ist (Virengefahr).
- ✓ SPAM-Mails werden immer häufiger auch zu kriminellen Zwecken eingesetzt (Phishing / Spear Phishing) mit dem Ziel, insbesondere personenbezogene Daten, Passwörter und Bankdaten durch Anklicken eines in der Spam-Mail enthaltenen Links zu erhalten!

Die E-Mail-Nutzung verlangt als herausragendes Kommunikationsmittel besondere Sorgfalt!



Praktizierter Datenschutz im Büroalltag

Regeln für die Nutzung freier Textfelder in Programmen

- ✓ Halten Sie nur objektiv Richtiges fest
- ✓ Vermeiden Sie persönliche Bewertungen
- ✓ Hinterlegen Sie grundsätzlich keine Angaben über Gesundheit, religiöse oder politische Einstellungen (es sei denn, es ist geschäftlich tatsächlich relevant)!

Der Betroffene – also auch der direkte Ansprechpartner beim Geschäftskunden – hat eine Recht auf Auskunft. Diese Auskunft umfasst alle Daten, die über den Betroffenen gespeichert sind und somit auch die hier gemeinten Bewertungen und Hinweise! Subjektive Bewertungen können rufschädigend sein und die gesamte Geschäftsbeziehung zerstören!



Fazit

- ✓ Kivitendo ist aus unserer Sicht geeignet, die Anforderungen des BDSG und die Vorgaben der kommenden EU-Grundschutzverordnung zu erfüllen, wenn bestimmte Punkte beachtet und Konzepte berücksichtigt werden
- ✓ Datenschutz bedeutet nicht nur gesetzliche Verpflichtung
- ✓ Die Beachtung der Regeln schafft Vertrauen
- ✓ Faustregel: Behandeln Sie die Daten anderer so, wie Sie selbst Ihre eigenen Daten behandelt wissen möchten!

Ihr betrieblicher Datenschutzbeauftragter steht Ihnen in allen Fragen rund um den Datenschutz mit Rat und Tat zur Verfügung. Sprechen Sie ihn lieber einmal zu oft als einmal zu wenig an.



Praktizierter Datenschutz im Büroalltag

Ihre Fragen?





Vielen Dank für Ihre
Aufmerksamkeit!

Ihr Ansprechpartner: Claus Wissing

WiR Solutions GmbH • Hansaring 26 • 48268 Greven
Tel.: 0800 - 2 333 333 • info@wir-solutions.de •
www.wir-solutions.de

