IT & LAW CONSULTING GMBH

Juristische Aspekte von Mobile Device Management

mag. iur. Maria Winkler

19. März 2014

Agenda

- **Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management**
- Gesetzliche Anforderungen an die Datensicherheit
- Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern
- Arbeitsrechtliche Aspekte
- Lizenzrechtliche Fragen
- Mobile Device Management Policy

Einführung

- Viele geschäftliche Aufgaben werden heute mit Mobile Devices erledigt – sie gehören heute oft zur „Arbeitsausrüstung“.
- Dies bringt diverse rechtlichen Fragen nach Sicherheit von Daten und Geschäftsgeheimnissen aber auch beispielsweise nach der Kontrolle von Mitarbeitenden und deren Zulässigkeit.

Begriffe

- Unter **Mobile Device Management** werden in der Regel die technischen, organisatorischen und auch arbeitsrechtlichen Massnahmen des Unternehmens im Zusammenhang mit der Nutzung von Mobile Devices (Smart Phones, Notebooks, etc.) durch die Arbeitnehmer verstanden – unabhängig davon, ob diese dem Unternehmen oder dem Arbeitnehmer gehören.
- „**Bring Your Own Device (BYOD)**“ bezeichnet die Nutzung der privaten Mobile Devices durch die Arbeitnehmer im Interesse und in der Regel auch innerhalb der Infrastruktur des Arbeitgebers.
- Im Folgenden werden beide Themen besprochen.

Mobile Device Management

- Mit der Verwendung von Mobile Devices (MD) entstehen im Unternehmen technische und rechtliche Risiken, welche häufig durch Weisungen (z.B. in einem IT-Nutzungsreglement) reduziert werden sollen.
- Beispiele für Risiken:
  - Verletzung von eigenen und fremden Geschäftsgeheimnissen bei der Verwendung von MD
  - Sicherheitsrisiken Zugriff auf die interne IT-Infrastruktur via MD
  - Private Nutzung der geschäftlichen MD
  - Durchsetzung von unternehmensweiten Sicherheitsvorgaben
  - etc.

BYOD

- Mitarbeiter greifen mit eigenen Smartphones, Tablet-PC‘s usw. auf die Unternehmensdaten und –infrastruktur zu.
- Das Arbeitsmittel wird dabei nicht vom Arbeitgeber zur Verfügung gestellt. Dies erfolgt meist auf Wunsch des Mitarbeitenden.
- Unternehmen ersparen sich mit BYOD Kosten für die Beschaffung der Geräte. Zudem folgen sie einem Trend – Mitarbeitende möchten mit ihren gewohnten Arbeitsmitteln arbeiten und private und geschäftliche Informationen nutzen können.
- Beide Seiten erhoffen sich in der Regel eine Effizienzsteigerung.

Risiken für den Arbeitgeber

- **Schutz der Unternehmens- und Kundendaten:**
  - Vermischung privater und geschäftlicher Informationen auf einem Gerät, das nicht der Kontrolle des Unternehmens unterliegt
  - Mangelnde Durchsetzung von Sicherheitsvorgaben
  - Zugriff unberechtigter Dritter auf das private Device
  - Die Daten des Unternehmens sind nach Beendigung des Arbeitsverhältnisses auf dem privaten Device vorhanden
  - Archivierung geschäftlicher E-Mails
- **Arbeitsrecht**
  - Anspruch auf Ersatz der Kosten des Mitarbeiters durch das Unternehmen
  - Kontrolle der Devices: Zugriff auf private Daten

Risiken für den Arbeitnehmer

- Vermischung von privaten und geschäftlichen Daten
- Zugriff des Arbeitgebers auf private Daten, welche auf dem Device gespeichert sind
- Löschung der privaten Daten durch den Arbeitgeber

Agenda

- Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management
- **Gesetzliche Anforderungen an die Datensicherheit**
- Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern
- Arbeitsrechtliche Aspekte
- Lizenzrechtliche Fragen
- Mobile Device Management Policy

Gesetzliche Grundlagen

- **Private und Bundesorgane**
  - Bundesgesetz über den Datenschutz (DSG, SR 235.1)
  - Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)

- **Kantonale und kommunale Behörden**
  - Kantonale Datenschutzgesetze

- Im Folgenden wird auf das Datenschutzgesetz des Bundes und hier auf die Bestimmungen für Private eingegangen.

Personendaten

- **Personendaten**
  alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen
- **besonders schützenswerte Personendaten**
  besondere Gefahr der Persönlichkeitsverletzung
  Angaben über:
  - religiöse, weltanschauliche oder politische Haltung
  - Intimsphäre, Gesundheit, ethnische Zugehörigkeit
  - Massnahmen der Sozialhilfe
  - administrative und strafrechtliche Massnahmen und Sanktionen

Persönlichkeitsprofil

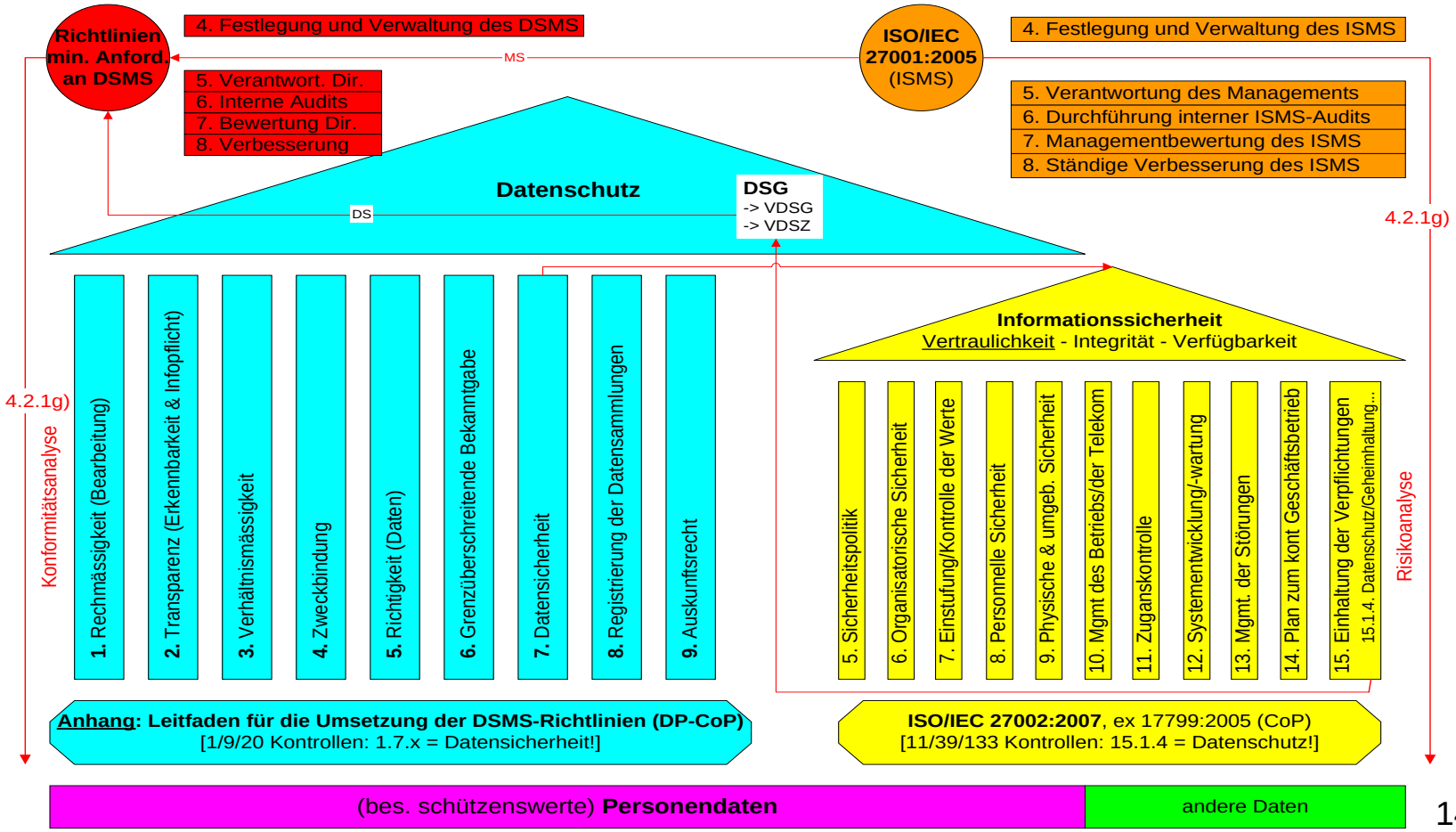
- **Persönlichkeitsprofile**
  Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt.
- Daten die über einen **längeren Zeitraum** zusammengetragen werden (Längsprofil) sind eher als Persönlichkeitsprofile zu qualifizieren als solche die eine Momentaufnahme (Querprofil) darstellen
- Voraussetzungen für Persönlichkeitsprofil:
  - Zusammenstellung mehrerer Informationen
  - über eine bestimmte/bestimmbare natürliche Person
  - Ermöglichung der Beurteilung wesentlicher Aspekte der Persönlichkeit
- Nur Geburtsdatum, Name, Adresse genügen nicht!

Bearbeiten von Personendaten

= jeder Umgang mit Personendaten

- Unabhängig von den angewendeten Mitteln und Verfahren
- Erheben, Beschaffen, Aufzeichnen, Sammeln, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Vernichten usw.
- Auch im Arbeitsverhältnis und bei der Arbeitsverrichtung durch den Mitarbeiter werden Personendaten bearbeitet.

Bearbeitungsprinzipien



Rechtmässigkeit

- **Bearbeitung durch Private**
  Datenbearbeitung ist grundsätzlich zulässig, ausser sie stellt eine widerrechtliche Verletzung der Persönlichkeit der betroffenen Person dar z.B. Bearbeitung entgegen den ausdrücklichen Willen der betroffenen Person; in diesem Fall muss ein **Rechtfertigungsgrund** (z.B. vertragliche Beziehungen (zB Arbeitsverhältnis oder Einwilligung) vorliegen.
- **Bearbeitung durch öffentliche Organe**
  Personendaten dürfen zur Erfüllung von Aufgaben bearbeitet werden, für die eine **Rechtsgrundlage** besteht (Legalitätsprinzip).

Transparenz und Einwilligung

- **Transparenz** (Art. 4 Abs. 4 DSG)
  - Die Beschaffung der Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person **erkennbar** sein.
  - Die Bearbeitung hat nach Treu und Glauben zu erfolgen (Gebot des loyalen, anständigen und korrekten Verhaltens).
- **Einwilligung** (Art. 4 Abs. 5 DSG)
  - Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese erst gültig, wenn sie **nach angemessener Information freiwillig** erfolgt.
  - Bei der Bearbeitung von besonders schützenswerten Personendaten muss sie zudem **ausdrücklich** erfolgen.

Verhältnismässigkeit u. Zweckbindung

- **Verhältnismässigkeit** (Art. 4 Abs. 2 DSG)
  - Bearbeitung nur soweit wie für Aufgabenerfüllung notwendig und geeignet
  - Beschränkung auf das Notwendige und tatsächlich Erforderliche
  - Nicht mehr benötigte Daten müssen vernichtet oder anonymisiert/ pseudonymisiert werden, sofern keine Archivierungs- oder Aufbewahrungspflicht bestehen
  - Keine Datensammlung auf Vorrat
- **Zweckbindung** (Art. 4 Abs. 3 DSG)
  - Verwendung der Daten nur zum vorgegebenen Zweck
  - Bei Zweckänderung muss die Einwilligung der betroffenen Person eingeholt werden

Datensicherheit

- Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG).
- Die Massnahmen werden in den Art. 8-12 VDSG konkretisiert.
- Der EDÖB hat einen **Leitfaden über die technischen und organisatorischen Massnahmen** publiziert (http://www.edoeb.admin.ch/dokumentation/00445/00472/00935/index.html?lang=de).

Datensicherheit

- Datensicherheit als wichtiges Grundelement des Datenschutzes.
- Ohne genügende Sicherheitsmassnahmen ist ein wirksamer Datenschutz nicht möglich.
- Im Gegensatz zum Datenschutz der die Persönlichkeit einer Person schützt gilt die Datensicherheit dem **Schutz der Informationen**.

Technische und organisatorische Massnahmen zur Datensicherheit

- In der Verordnung zum Datenschutzgesetz (VDSG) werden die zu treffenden Massnahmen konkretisiert.
- Es werden die folgenden Themen geregelt:
  - Allgemeine Massnahmen
  - Besondere Massnahmen
  - Protokollierungen
  - Bearbeitungsreglement
  - Bekanntgabe der Daten

Allgemeine Massnahmen (Art. 8 VDSG)

Wer als **Privatperson** Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die **Vertraulichkeit**, die **Verfügbarkeit** und die **Integrität** der Daten, um einen angemessenen Datenschutz zu gewährleisten.

Insbesondere schützt er die Systeme gegen folgende **Risiken**:

a. unbefugte oder zufällige Vernichtung;

b. zufälligen Verlust;

c. technische Fehler;

d. Fälschung, Diebstahl oder widerrechtliche Verwendung;

e. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

Allgemeine Massnahmen (Art. 8 VDSG)

Die technischen und organisatorischen Massnahmen müssen **angemessen** sein.

Insbesondere tragen sie folgenden Kriterien Rechnung:

a. Zweck der Datenbearbeitung;

b. Art und Umfang der Datenbearbeitung;

c. Einschätzung der möglichen Risiken für die betroffenen Personen;

d. Gegenwärtiger Stand der Technik.

Diese Massnahmen sind periodisch zu überprüfen.

Besondere Massnahmen (Art. 9 VDSG)

- Zugangskontrolle (Bsp. eigener Schlüssel)
- Personendatenträgerkontrolle (Bsp. Memory-Stick)
- **Transportkontrolle** (Bsp. verschlüsselte Kommunikation über Internet)
- **Bekanntgabekontrolle** (Bsp. Identifikation der Datenempfänger), Speicherkontrolle (Bsp. Eingabe in den Datenspeicher)
- Benutzerkontrolle (Bsp. Verhinderung des Eindringens in Datennetz)
- Zugriffskontrolle
- Eingabekontrolle (Bsp. Protokollierungen)

Protokollierung (Art. 10 VDSG)

- Der Inhaber der Datensammlung protokolliert die **automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen**, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können. Eine Protokollierung hat insbesondere dann zu erfolgen, wenn sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Der Beauftragte kann die Protokollierung auch für andere Bearbeitungen empfehlen.
- Die Protokolle sind **während eines Jahres revisionsgerecht festzuhalten**. Sie sind ausschliesslich den Organen oder privaten Personen zugänglich, denen die Überwachung der Datenschutzvorschriften obliegt, und dürfen nur für diesen Zweck verwendet werden.

Protokollierung

- Die Protokollierung ist nur dann zwingend, wenn es sich um eine automatisierte Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen handelt und wenn die anderen Schutzmassnahmen nicht ausreichen.
- Protokollierungen können generell sinnvoll sein, um nachvollziehen zu können, wer wann was gemacht hat (Leistungskontrolle, Nachvollziehbarkeit der unternehmerischen Abläufe, etc.).
- Protokollierungsmassnahmen müssen zweck- und verhältnismässig sein. Der Zugriff auf die Protokolle muss restriktiv gehandhabt werden.

Bearbeitungsreglement (Art. 11 VDSG)

- Der Inhaber einer meldepflichtigen automatisierten Datensammlung (Art. 11*a* Abs. 3 DSG), die nicht aufgrund von Artikel 11*a* Absatz 5 Buchstaben b–d DSG von der Meldepflicht ausgenommen ist, erstellt ein Bearbeitungsreglement, das insbesondere die **interne Organisation** sowie das **Datenbearbeitungs- und Kontrollverfahren** umschreibt und die Unterlagen über die **Planung, die Realisierung und den Betrieb der Datensammlung und der Informatikmittel** enthält.
- Der Inhaber der Datensammlung **aktualisiert** das Reglement regelmässig. Er stellt es dem Beauftragten oder dem Datenschutzverantwortlichen nach Artikel 11*a* Absatz 5 Buchstabe e DSG auf Anfrage in einer für sie verständlichen Form zur Verfügung.

Meldepflicht (Art. 11a DSG)

- Private Personen müssen Datensammlungen anmelden, wenn
  - Regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden
  - Regelmässig Personendaten an Dritte bekannt gegeben werden
- Datensammlungen sind beim EDÖB anzumelden, bevor die Datensammlung eröffnet wird. Dieser führt ein **Register** der angemeldeten Datensammlungen, das über das Internet zugänglich ist.

Ausnahmen von der Meldepflicht

- Eine Ausnahme besteht insbesondere dann, wenn
  - Personendaten aufgrund **gesetzlichen Verpflichtung** bearbeitet werden.
  - ein Datenschutzverantwortlicher bezeichnet wird, **der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis** der Datensammlungen führt.
  - aufgrund eines Zertifizierungsverfahrens ein **Datenschutzqualitätszeichen** erworben wird und das Ergebnis der Bewertung dem Beauftragten mitgeteilt wird.
- Der **Bundesrat** hat noch weitere Ausnahmen ausdrücklich festgelegt (z.B. archivierte Daten, Buchhaltungsunterlagen, etc.).

Datenschutzverantwortlicher

- Wenn das Unternehmen einen Datenschutzverantwortlichen benennt, dann muss es seine Datensammlungen nicht mehr dem EDÖB melden.
- Dieser darf keine anderen Tätigkeiten ausüben, welche mit seinen Aufgaben als Datenschutzbeauftragter unvereinbar sind und muss über die notwendigen Fachkenntnisse verfügen.
- Der Datenschutzverantwortliche ist, entgegen seiner Bezeichnung, nicht dafür verantwortlich, wenn das Unternehmen Datenschutzverletzungen begeht - die **Verantwortung bleibt beim Unternehmen**!
- Die Bezeichnung eines Datenschutzverantwortlichen kann auch als eine Massnahme zur Gewährleistung der Datensicherheit im Sinn von Art. 7 DSG erforderlich sein!

Zwischenfazit

- Das Datenschutzgesetz schützt die Daten von natürlichen und von juristischen Personen.
- Es stellt grundsätzliche Anforderungen an die Bearbeitung von Personendaten und verlangt insbesondere auch, dass **angemessene technische und organisatorische Massnahmen** zu deren Schutz ergriffen werden.
- Das DSG und die VDSG geben allgemeine Leitlinien vor, die im Leitfaden des EDÖB über die technischen und organisatorischen Massnahmen genauer ausgeführt werden.
- Die konkreten Auswirkungen auf das MDM werden im Folgenden besprochen.

Relevante Sicherheitsrisiken

- Zu den Risiken zählen insbesondere:
  - Verletzung von **Geschäftsgeheimnissen**
  - **Datenschutzverletzungen**
  - **Datenverlust** durch Diebstahl oder Verlust des Geräts
  - **Zugriff unberechtigter Dritter** auf das Gerät
  - **Vermischung** von geschäftlichen und privaten Daten
  - Mangelnde Kontrolle und Durchsetzung der **Sicherheitsvorgaben** des Unternehmens (Virenschutz, etc)
  - Kontrollverlust über das Gerät (BYOD)
  - **Mobile Malware** (Mikrofon, Kamera, Backdoors, etc)
  - **Backup** der Daten
  - etc.

Massnahmen

- Die Speicherung und Bearbeitung von Geschäftsdaten wie Daten von Kunden, Lieferanten und Mitarbeitenden mit mobilen Devices bringt zusätzliche Sicherheitsrisiken mit sich, denen durch entsprechende **angemessene** technische und organisatorische Massnahmen begegnet werden muss.
- Die Massnahmen des Unternehmens im Zusammenhang mit Mobile Device Management sollten im Einklang mit der Erhebung mindestens der folgenden Risiken erfolgen:
  - Schutzbedarf der Daten, auf welche zugegriffen wird
  - Bestehende Sicherheitsvorgaben und Sicherheitsbedürfnisse
  - Arbeitsrechtliche Risiken

Massnahmen

- Infrage kommen technische und organisatorische Massnahmen wie
  - Klassifizierung der Daten
  - Restriktive Erteilung von Zugriffsberechtigungen auf die eigenen Systeme und Daten je nach Klassifizierung
  - Verschlüsselung von Daten, und Kommunikationswegen
  - Überwachung der MD mittels entsprechender Software
  - Überwachung der Mitarbeitenden
  - Vertragliche Geheimhaltungsvereinbarungen
  - Sicherheitskonzepte
  - Erlass von Weisungen und Policies, etc.
- Dabei sind die rechtlichen Rahmenbedingungen zu beachten!

Anonymisierung, Pseudonymisierung, Verschlüsselung

- Gemäss Leitfaden des EDÖB gilt bei der Bearbeitung von Personendaten, dass vorzugsweise anonymisierte Daten verwendet werden sollten, **wenn es der Zweck der Datenbearbeitung zulässt**. Dadurch verringern sich die Anforderungen an die technischen und organisatorischen Massnahmen.
- Wenn eine Anonymisierung nicht möglich sein sollte, so sollten die Daten möglichst **pseudonymisiert** werden.
- Wenn auch eine Pseudonymisierung im Hinblick auf den Zweck der Bearbeitung **nicht möglich** sein sollte, so sollten zumindest die besonders schützenswerten Personendaten **verschlüsselt** (gespeichert) werden.

Anonymisierung und Pseudonymisierung

- Daten sind dann **anonymisiert**, wenn die Herstellung eines Personenbezugs generell nicht mehr möglich ist. In diesem Fall **handelt es sich nicht mehr um Personendaten** und das Datenschutzgesetz ist nicht mehr anwendbar.
- Bei der **Pseudonymisierung** werden alle Daten, die Rückschlüsse auf die konkrete Person zulassen, durch **neutrale Angaben (Pseudonym)** ersetzt. Aus einer Tabelle lässt sich nachvollziehen, welches Pseudonym (z.B. eine Nummer) zu welcher Person gehört. Solange die Tabelle existiert, kann die Pseudonymisierung wieder rückgängig gemacht werden.
- Die Tabelle darf nur berechtigten Personen zugänglich sein!

Verschlüsselung

- Gemäss herrschender Literatur und Lehrmeinung ist eine Verschlüsselung auch bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen nicht zwingend, wenn ein angemessener Schutz durch andere Massnahmen gewährleistet werden kann.
- Generell stellt sich die Frage, **ob es sich bei verschlüsselten Daten überhaupt noch um Personendaten handelt**, da die Herstellung des Personenbezugs nicht möglich ist.
- Hier besteht keine eindeutige und einhellige Lehrmeinung, weshalb grundsätzlich davon ausgegangen werden sollte, dass auch bei verschlüsselten Daten das Datenschutzgesetz zu beachten ist.
- Der Chiffrierschlüssel muss gesichert werden und es dürfen nur wenige Personen darauf Zugriff haben.

Empfehlung

- Abhängig vom Schutzbedarf der Daten müssen die technischen Massnahmen ergriffen werden, welche geeignet sind, ein **angemessenes Schutzniveau** herzustellen.
- Dies sind neben der Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten auch die Regelung der Zugriffsberechtigungen und des physischen Zutritts zu Serverräumen oder die Verhinderung des Datenexports (z.B. per E-Mail oder USB, etc.)
- Zusätzlich müssen organisatorische Massnahmen ergriffen werden – einige werden im Folgenden besprochen.

Organisatorische Massnahmen

- Als geeignete organisatorische Massnahmen kommen insbesondere der Erlass von Weisungen und Policies, die Beschränkung der Zugriffe auf Daten mittels MD, die Schulung von Mitarbeitenden, die Kontrolle der Datenbearbeitungen, der Abschluss von Vertraulichkeitsvereinbarungen etc. in Betracht.
- Im Folgenden werden die folgenden Themen erörtert:
  - Überwachung der Mitarbeitenden
  - Erlass von Policies

Agenda

- Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management
- Gesetzliche Anforderungen an die Datensicherheit
- **Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern**
- Arbeitsrechtliche Aspekte
- Lizenzrechtliche Fragen
- Mobile Device Management Policy

Datenbearbeitung durch den Arbeitgeber

- Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen **Eignung für das Arbeitsverhältnis** betreffen oder zur **Durchführung des Arbeitsvertrages** erforderlich sind (Art. 328b OR).
- Es dürfen nur die Daten der Arbeitnehmer bearbeitet werden, die **objektiv nötig** sind, um ein berechtigtes Interesse des Arbeitgebers oder des Arbeitnehmers zu erfüllen. Nötig bedeutet gemäss Rosenthal aber nicht absolut unabdingbar, sondern **vernünftigerweise geboten** (Handkommentar zum Datenschutzgesetz, 2008).
- Folge: Persönliche Verhältnisse, Eigenschaften und Neigungen, die nicht wesentlich die beruflichen Fähigkeiten mitbestimmen, gehen den Arbeitgeber nichts an und dürfen von diesem weder erfragt noch gespeichert werden.

Erlaubte Datenbearbeitung

- Der Arbeitgeber kann in zwei Fällen und in einem bestimmten Umfang Daten über Angestellte bearbeiten:
  - **Vor dem Abschluss eines Arbeitsvertrags und während seiner Durchführung** dürfen Daten über Bewerbende bearbeitet werden, um abzuklären, ob sie für die betreffende Arbeitsstelle geeignet sind.
  - **Während der Anstellung** dürfen diejenigen Daten über Angestellte bearbeitet werden, die für die Durchführung des Arbeitsverhältnisses erforderlich sind.

Rechte und Pflichten

Arbeitgeber

- Allgemeine **Fürsorgepflicht** (Art. 328 OR)
- insbesondere **Schutz der Persönlichkeit** bei der Bearbeitung von Personendaten (Art. 328b OR)- Bundesgesetz über den Datenschutz (SR 235.1)
- **Verbot der Verhaltensüberwachung** (ArGV 3, SR 822.113)
- **Weisungsrecht** (Art. 321d OR)

Arbeitnehmer

- Sorgfalts – und **Treuepflicht** (Art. 321a OR)
- Sorgfältiger Umgang mit Arbeitsgeräten und technischen Einrichtungen, etc.

Aufzeichnung und Auswertung von Nutzungsdaten

- In Unternehmen werden zu verschiedenen Zwecken Daten über die Nutzung von IT-Systemen aufgezeichnet und ausgewertet, beispielsweise
  - zur Gewährleistung der Datensicherheit (Security)
  - zur Herstellung von Backups
  - zur Verrechnung von Leistungen
  - zur Kontrolle von Datenzugriffen
  - zur Kontrolle der Einhaltung eines Nutzungsreglements.
- Aufgezeichnet werden entweder nur die Randdaten (wer hat wann was gemacht) oder auch die Inhalte.

Überwachungs- und Kontrollsysteme am Arbeitsplatz

- Überwachungs- und Kontrollsysteme, die das **Verhalten** der Arbeitnehmer am Arbeitsplatz **überwachen** sollen, sind **verboten** (Art. 26 der Verordnung 3 zum Arbeitsgesetz).
- Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich, sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt werden (Verhältnismässigkeitsprinzip).
- **Erlaubt** sind solche Systeme aus **Sicherheitsgründen** und zur **Erfassung der Arbeitsleistung**.
- Beispiele: Telefonzentralen (Überwachung ein- und ausgehender Anrufe, etc.), EDV-Systeme (Anzahl Anschläge pro Minute bei Textverarbeitung, wann der Rechner benutzt wird, etc.)

Bundesgerichtsurteil 8C_448/2012

- Das Bundegericht beurteilte eine fristlose Kündigung eines Mitarbeitenden wegen Missbrauchs der Informatikanlage als ungerechtfertigt, weil die Beweise mit Hilfe eines **heimlich installierten Überwachungs-Programms** erhoben wurden.
- Mithilfe des Programms konnte nachgewiesen werden, dass der Mitarbeitende einen erheblichen Teil seiner Arbeitszeit für private oder geschäftsfremde Zwecke verwendete.
- Das Programm erstellte Screenshots, daher konnte der Arbeitgeber auch Kenntnisse vom Inhalt der besuchten Websites erlangen. Diese waren zum Teil streng vertraulich (e-Banking, privat oder unterlagen dem Amtsgeheimnis).
- Die Überwachung widerspricht Art. 26 Abs. 1 der Verordnung 3 des ArG, daher sind die Beweise nicht verwertbar.

Überwachung aus Sicherheitsgründen

- Beim Einsatz von Überwachungssystemen aus Sicherheitsgründen muss eine für die Arbeitnehmenden möglichst schonende Vorgehensweise gewählt werden.
- Beispiel Diebstahlüberwachung durch Videoüberwachung am Arbeitsplatz: Es soll möglichst verhindert werden, dass die gewählten Bildausschnitte die Angestellten erfassen.
- Alternative Möglichkeiten sind zu prüfen.

Internet- und E-Mailnutzung am Arbeitsplatz

- Bei der Nutzung von Internet und E-Mail am Arbeitsplatz bestehen teilweise divergierende Interessen des Arbeitgebers und der Mitarbeitenden.
- Überwachungsmassnahmen müssen unter Beachtung der arbeits- und datenschutzrechtlichen Grundsätze implementiert werden!

Interesse Arbeitgeber - Arbeitnehmer

Arbeitgeber Interessen

- Zugriff auf geschäftliche Informationen
- Vermeidung übermässiger Belastung der Ressourcen durch private Nutzung
- Archivierung
- Beweissicherung
- Transparenz
- **Überwachung der Mitarbeitenden**

Arbeitnehmer Interessen

- Nutzung von E-Mail und Internet zu privaten Zwecken
- **Schutz der Persönlichkeit**
- **Transparenz** betreffend Überwachung

Rechtliche Voraussetzungen für die Überwachung

- Erlaubt sind permanente anonymisierte Auswertungen von Protokollierungen sowie stichprobenartige pseudonymisierte Auswertungen der Protokollierungen, um zu überprüfen, ob das Nutzungsreglement eingehalten wird.
- Um eine personenbezogene Überwachung einleiten zu dürfen braucht es
  1. **die vorherige Information der Mitarbeitenden**
     - Bestehen eines Überwachungsreglements
  2. **Feststellung eines Missbrauchs oder Bestehen eines konkreten Missbrauchsverdachts**
     - z.B. Verletzung Nutzungsreglements (z.B. Surfen auf Web-Seiten, die keine berufliche Relevanz aufweisen)

Missbrauch

- Als Missbrauch ist nicht nur eine Zuwiderhandlung gegen eine konkrete Bestimmung im Nutzungsreglement zu qualifizieren – auch wenn kein Nutzungsreglement besteht, ist z.B. das übermässige private Mailen oder Surfen als Missbrauch zu werten.
- Der Verdacht muss **konkret** sein – die blosse Wahrscheinlichkeit genügt nicht.
- Der Verdacht muss sich aber **nicht bereits auf eine bestimmte Person** beziehen.
- Wie der Verdacht entstanden ist, ist unerheblich – auch eine Beobachtung des Vorgesetzten oder der anderen Mitarbeitenden genügt.

Weiter erlaubt …

- die personenbezogene Auswertung der Nutzerdaten zur Behebung von Störungen zur Abwehr einer konkreten Bedrohung;
- das Scanning von E-Mails durch ein Virenprogramm;
- die personenbezogene Auswertung zur Fakturierung von Leistungen

Private E-Mails

- Private Post, dazu zählen auch E-Mails, geniessen auch am Arbeitsplatz uneingeschränkten Schutz. Private Post ist ungeöffnet an die adressierte Person weiterzuleiten.
- Auch wenn die private Nutzung von E-Mail erlaubt ist, kann das Unternehmen von der geschäftlichen Natur eines E-Mails ausgehen, wenn kein Unterscheidungsvermerk besteht (Kennzeichnung als persönlich oder privat) und die private Natur des E-Mails nicht erkennbar ist.
- Die Mitarbeitenden sind daher anzuhalten, private E-Mails als privat zu kennzeichnen und in separaten Ordnern oder auf separaten Datenträgern abzulegen.
- Darf E-Mail nur geschäftlich genutzt werden, dann dürfen alle E-Mails automatisch protokolliert und gespeichert werden.

Empfehlungen I

- Vor der Einführung von Überwachungsmassnahmen soll überprüft werden, ob das unerwünschte Verhalten nicht durch **technische oderorganisatorische Massnahmen** verhindert werden kann (z.B. Sperren von Websites, Schulungen, etc).
- Um Klarheit zu schaffen, sollte in einer **Weisung** die erlaubte und die verbotene Nutzung der technischen Infrastruktur geregelt werden (freiwillig).
- Die Mitarbeitenden müssen über die Tatsache, dass überwacht werden kann sowie über das grundsätzliche Vorgehen informiert werden (obligatorisches **Überwachungsreglement**).
- Überwachungsmassnahmen, die ausschliesslich dem Zweck der **Verhaltensüberwachung** dienen, sind verboten!

Empfehlungen II

- Bei Überwachungsmassnahmen sollte prinzipiell nach dem **Verhältnismässigkeitsgrundsatz** vorgegangen werden:
  - Der Zweck der Überwachungsmassnahme muss festgelegt werden.
  - Ausgehend davon sind nur die Massnahmen einzuleiten, welche tatsächlich erforderlich sind und die den geringsten Eingriff in die Persönlichkeitsrechte der Mitarbeitenden darstellen!
- Im Rahmen von anonymen Auswertungen von Protokollierungen darf überprüft werden, ob die Weisung eingehalten wird.
- Personenbezogene Auswertungen nur bei konkretem Missbrauchsverdacht!

Überwachung mit MDM Software

- Mittels MDM-Software greift das Unternehmen auf das mobile Device zu und kontrolliert dieses.
- Damit die Kontrolle zulässig ist, sollten folgende Punkte beachtet werden:
  - Die Mitarbeitenden müssen wissen, dass das MD kontrolliert wird.
  - Die geschäftlichen und die privaten Informationen sollten auf dem MD getrennt sein, sodass eine Löschung nur der geschäftlichen Informationen möglich ist.
  - Es muss transparent geregelt werden, was kontrolliert wird.
  - Die Kontrolle muss verhältnismässig sein.
  - Es muss klar geregelt werden, wann welche Daten gelöscht werden.

Einwilligung

- Möchte das Unternehmen im Zusammenhang mit BYOD die privaten Devices der Mitarbeitenden mittels MDM-Software überwachen, dann ist dazu die Einwilligung der betroffenen Person erforderlich.
- Ebenso ist eine Einwilligung erforderlich, wenn die private Nutzung der geschäftlichen Devices erlaubt ist und der Zugriff mittels MDM-Software nicht auf die geschäftlichen Daten beschränkt ist.

Einwilligungserklärung

- In der Praxis erfolgt das Einholen von Einwilligungen oft im Rahmen von **Policies**, deren Erhalt die Mitarbeitenden bestätigen.
- Dabei muss klar geregelt werden, auf welche Daten das Unternehmen Zugriff hat, dass das Gerät überwacht wird und unter welchen Voraussetzungen Daten (auch private) gelöscht werden.
- Im Rahmen von BYOD kann das Unterzeichnen einer Einwilligungserklärung auch als Voraussetzung für die Bewilligung zur Nutzung des privaten Devices für geschäftliche Zwecke erklärt werden. Wird die Einwilligung zurückgezogen, dann dürfen mit dem Device keine Geschäftsdaten mehr synchronisiert werden.

Mitarbeiterüberwachung

Publikationen des EDÖB

- **Bearbeitung von Personendaten im Arbeitsbereich**
  http://www.edoeb.admin.ch/themen/00794/00917/index.html?lang=de
- **Leitfaden betreffend Internet- und E-Mail-Überwachung**
  http://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=de

Agenda

- Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management
- Gesetzliche Anforderungen an die Datensicherheit
- Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern
- **Arbeitsrechtliche Aspekte**
- Lizenzrechtliche Fragen
- Mobile Device Management Policy

Arbeitsrechtliche Aspekte von MDM

- Bei der Nutzung von mobilen Devices und insbesondere bei BYOD sollten auch die folgenden arbeitsrechtlichen Themen ausreichend berücksichtigt werden:
  - Weisungsrecht des Arbeitgebers
  - Pflicht zur Kontrolle der Arbeitszeit
  - Ersatz der Auslagen bei BYOD

Weisungsrecht des Arbeitgebers

(Art. 321d OR)

- Es gibt dem Arbeitgeber die Befugnis zum Erlass von **allgemeinen Weisungen** wie zB eine MDM Policy oder aber auch **besonderen Weisungen** an einzelne Arbeitnehmer.
- Aufgrund des Subordinationsverhätlnisses untersteht der Arbeitnehmer einer Befolgungspflicht für gesetzlich zulässige Weisungen.
- Bei Nichtbefolgung kann der Arbeitgeber Disziplinarmassnahmen (Verwarnungen, Verweise, Erlasse etc.) aussprechen. Weitere Disziplinarmassnahmen wie Lohnkürzungen etc. bedürfen einer entsprechenden Verankerung im Arbeitsvertrag.

Treuepflicht

- Mitarbeitende haben die ihnen übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren (**Treuepflicht**, Art. 321 a OR).
- Die ihnen zur Verfügung gestellten Arbeitsgeräte müssen sie sorgfältig behandeln, sie dürfen den Arbeitgeber nicht konkurrenzieren und sind verpflichtet, Geschäfts- und Fabrikationsgeheimnisse schützen (Art. 321a OR).
- Zudem sind sie verpflichtet, die Weisungen des Arbeitgebers zu befolgen (Art. 321d Abs. 2 OR).

Verantwortung der Mitarbeitenden

- Sie **haften** für den Schaden, welchen sie dem Arbeitgeber zufügen (Art. 321e OR). Allerdings wird dabei vorausgesetzt, dass man dem betroffenen Mitarbeitenden tatsächlich auf Grund seiner Ausbildung, Erfahrung etc. einen Vorwurf machen kann.
- Der Arbeitgeber muss daher die Mitarbeitenden sorgfältig auswählen und instruieren – z.B. mittels Weisungen.
- Der Erlass einer MDM-Policy dient dem Arbeitgeber daher auch dazu, nachweisen zu können, dass er die Mitarbeitenden im Hinblick auf die Risiken, die mit der Nutzung von MD verbunden sind, ausreichend instruiert hat.

Kontrolle der Arbeitszeit

- Die durch den Einsatz von MD geförderte ständige Erreichbarkeit der Mitarbeitenden führt (unabhängig davon, wem die Geräte gehören), zu arbeitsrechtlichen Risiken des Unternehmens.
- Der Arbeitgeber ist verpflichtet, die Arbeitszeit der Mitarbeitenden zu erfassen (Art. 46 ArG i.V.m. Art. 73 ArGV 1).
- Liegt keine Arbeitszeiterfassung vor, dann besteht das praktische Risiko, dass das Unternehmen in einem Prozess um **Nachzahlung von Überstunden und Überzeit** verliert.

Pflicht zur Kontrolle der Arbeitszeit

- Der Arbeitgeber ist verpflichtet, die Arbeitszeit der Mitarbeitenden zu erfassen (Art. 46 ArG i.V.m. Art. 73 ArGV 1).
- Erfasst werden müssen beispielsweise

  die geleistete (tägliche und wöchentliche) Arbeitszeit inkl. Ausgleichs- und Überzeitarbeit sowie ihre Lage; die gewährten wöchentlichen Ruhe- oder Ersatzruhetage, soweit diese nicht regelmässig auf einen Sonntag fallen; die Lage und Dauer der Pausen von einer halben Stunde und mehr; die betrieblichen Abweichungen von der Tag-, Nacht- und Sonntagsdefinition nach den Artikeln 10, 16 und 18 des Gesetzes; Regelungen über den Zeitzuschlag nach Artikel 17b Absätze 2 und 3 des Gesetzes
- Diese Unterlagen müssen 5 Jahre aufbewahrt werden.

Ausnahmen

- Das Arbeitsgesetz ist nicht anwendbar auf Personen, die eine **höhere leitende Tätigkeit** oder eine wissenschaftliche oder selbständige künstlerische Tätigkeit ausüben (Art. 3 Bst. d ArG).
- Eine höhere leitenden Tätigkeit hat nur derjenige, der über **weitreichende Entscheidungsbefugnisse** verfügt oder zumindest Entscheidungen von grosser Tragweite **massgebend beeinflussen** kann.
- Unternehmen müssen daher die Arbeitszeit aller Mitarbeitenden, bis auf wenige Ausnahmen, kontrollieren.
- Die Pflicht zur **Erfassung** der Arbeitszeit kann an den Mitarbeitenden delegiert werden, die **Verantwortung** bleibt beim Unternehmen.

Folgen bei Verletzung

- Zuwiderhandlungen gegen Art. 46 ArG sind nicht direkt sanktioniert, unterliegen aber dem Verwaltungszwang (Art. 51 und 52 ArG), eventuell in Verbindung mit einer Ungehorsamstrafe (Art. 292 StGB).
- Das wesentliche Risiko für die Unternehmen besteht aber darin, dass es in einem Prozess betreffend die Geltendmachung von Überstunden und Überzeit verlieren kann, wenn es seiner Verantwortung zur Kontrolle der Arbeitszeit nicht nachgekommen ist!

Neue Weisung des Seco

- Seit 01.01.2014 gilt eine neue Weisung des Seco, welche sich an die kantonalen Arbeitsinspektoren richtet.
- Es müssen neu nicht mehr bei allen Arbeitnehmern alle Informationen erfasst werden – unerlässlich ist aber weiterhin die Dokumentation der täglichen und wöchentlichen Arbeitszeit.
- Es gibt nun 3 Kategorien von Arbeitnehmenden:
  - Keine Arbeitszeiterfassung (Top-Manager)
  - Vereinfachte Arbeitszeiterfassung
  - Arbeitszeiterfassung gemäss Art. 73 ArGV 1

Vereinfachte Arbeitszeiterfassung

- Arbeitnehmer, die einen **wesentlichen Entscheidungsspielraum** in der Arbeit haben, ihre **Arbeit weitgehend selbst planen** und auch **selbst entscheiden, wann sie arbeiten**, kann eine vereinfachte Arbeitszeiterfassung vorgenommen werden – Voraussetzung ist allerdings, dass sie nicht regelmässig Nacht- und Sonntagsarbeit leisten.
- Für diese Arbeitnehmer spielt die **transparente Information des Arbeitgebers**, welche **Zeitrahmen** und **Ruhezeiten** einzuhalten sind, nach Meinung des Seco eine grössere Rolle.
- Sie müssen aber ihre tägliche und wöchentliche Arbeitszeit dokumentieren.
- Dies gilt nur, wenn eine **Vereinbarung** mit dem Arbeitgeber besteht, in der der Arbeitnehmer auf die lückenlose Erfassung verzichtet.

Empfehlung

- Durch den Einsatz von MD in Unternehmen ist die Kontrolle der Arbeitszeit schwieriger – das Unternehmen kann nicht oder nur schwer kontrollieren, wann die Mitarbeitenden Mails beantworten, etc.
- Es sollte klar geregelt werden, welche Arbeitszeiten einzuhalten sind.
- Den Mitarbeitenden muss eine Möglichkeit zur Erfassung der Arbeitszeit gegeben werden.

Kostenersatz

- Der Arbeitgeber hat den Arbeitnehmer mit den Geräten und dem Material auszurüsten, das für die Ausführung der Arbeit erforderlich ist.
- Stellt im Einverständnis mit dem Arbeitgeber der Arbeitnehmer selbst Geräte oder Material für die Ausführung der Arbeit zur Verfügung, so ist er dafür angemessen zu entschädigen, sofern nichts anderes verabredet oder üblich ist (Art. 327 OR).

Kostenersatz bei BYOD

- Wenn der Mitarbeitende sein eigenes Device für die Erledigung geschäftlicher Aufgaben verwendet, dann muss ihm das Unternehmen die Kosten ersetzen.
- Dies kann entweder durch eine pauschale Entschädigung, sofern diese tatsächlich alle Kosten deckt, erfolgen oder individuell abgerechnet werden.
- Die Kostenregelung sollte schriftlich festgehalten werden.
- Zu beachten gilt es nebst den regelmässig anfallenden Kosten weitere Kosten wie Abschreibung, Wertverlust, Maintenance und Support etc.

Agenda

- Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management
- Gesetzliche Anforderungen an die Datensicherheit
- Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern
- Arbeitsrechtliche Aspekte
- **Lizenzrechtliche Fragen**
- Mobile Device Management Policy

Urheberrecht

- Das Urheberrecht schützt Werke; es muss sich dabei um eine geistige Schöpfung in Literatur und Kund mit individuellem Charakter handeln (Art. 2 Abs. 1 URG).
- Computerprogramme sind keine Werke, werden diesen aber in Art. 2 Abs. 3 URG gleichgestellt.
- Computerprogramme sind alle in einer Programmiersprache verfassten Verfahren zur Lösung einer Aufgabe, inklusive die entsprechende Dokumentation. Darunter fallen auch Programme in die in Hardware integriert sind, jene mit konkreter Nutzanwendung sowie auch spielerische Programme.

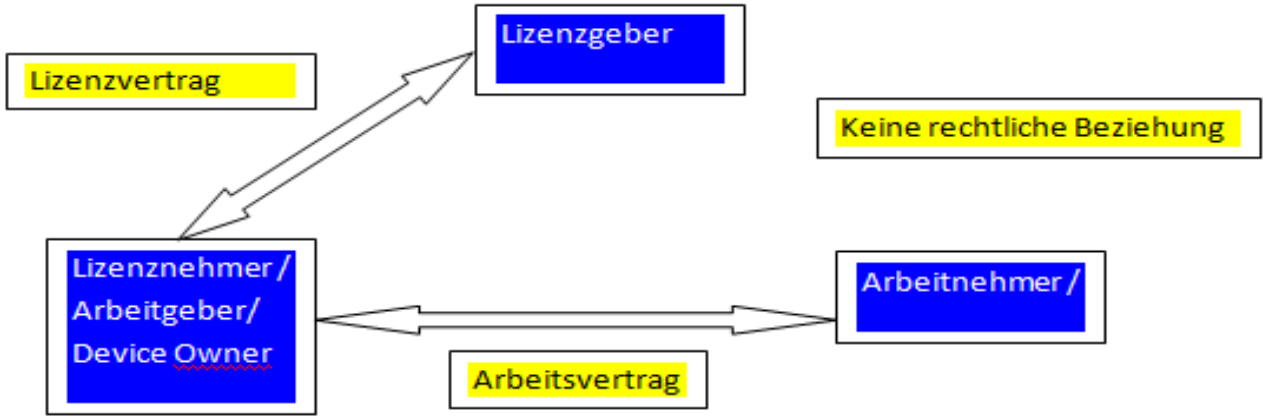
Urheberrecht

- Das Urheberrecht zählt zu den Immaterialgüterrechten. Urheber ist die natürliche Person, die das Werk geschaffen hat.
- Diejenige Person, welche auf dem Werk als Urheber genannt wird, gilt nach gesetzlicher Vermutung als Urheber!
- Der Urheber hat das ausschliessliche Recht am eigenen Werk - er darf z.B. bestimmen, ob es veröffentlicht werden darf, ob es im Internet frei oder unter bestimmten Auflagen verwendet werden darf, etc.
- Eine Verletzung des Urheberrechts ist **strafbar**!

Lizenzrechte

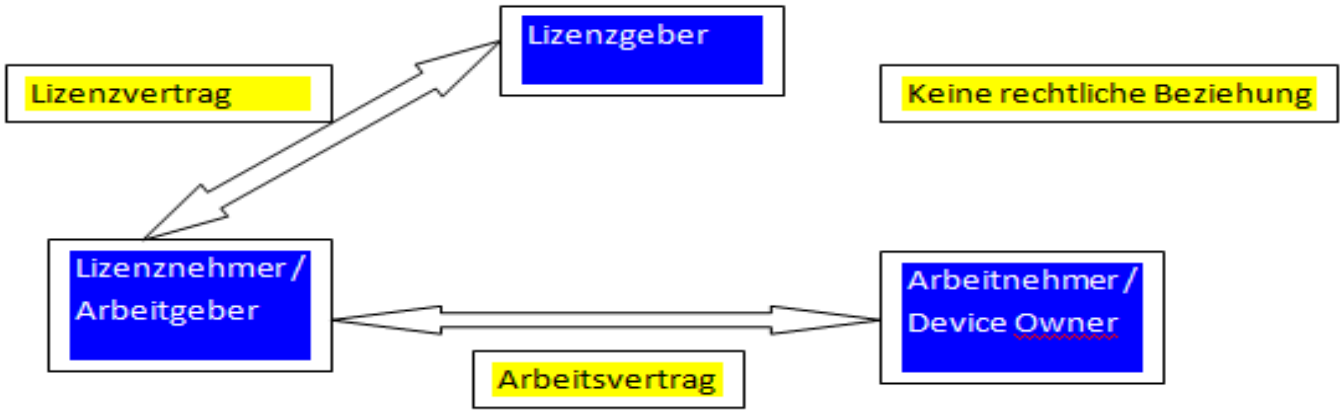
- Mit deiner Lizenz räumt der Inhaber eines Rechts **Nutzungsrechte** in einem bestimmten Rahmen ein.
- Objekte von Lizenzverträgen können urheberrechtliche Werke, somit auch Computerprogramme sein. Eine Lizenz kann auch an einer Marke, einem Label und anderen immaterialgüterrechtlich geschützten Bereichen vergeben werden.
- Im Geschäftsalltag betreffen Lizenzen meist Software oder Marken.
- Werden im Rahmen von BYOD geschäftliche Programme auf den privaten Devices eingesetzt, dann kann dies gegen den Lizenzvertrag verstossen.
- Es sollte dringend kontrolliert werden, ob und wenn ja unter welchen Voraussetzungen Programme, welche durch das Unternehmen lizenziert wurden, auch auf privaten Devices eingesetzt werden dürfen.

Lizenzrechte MDM



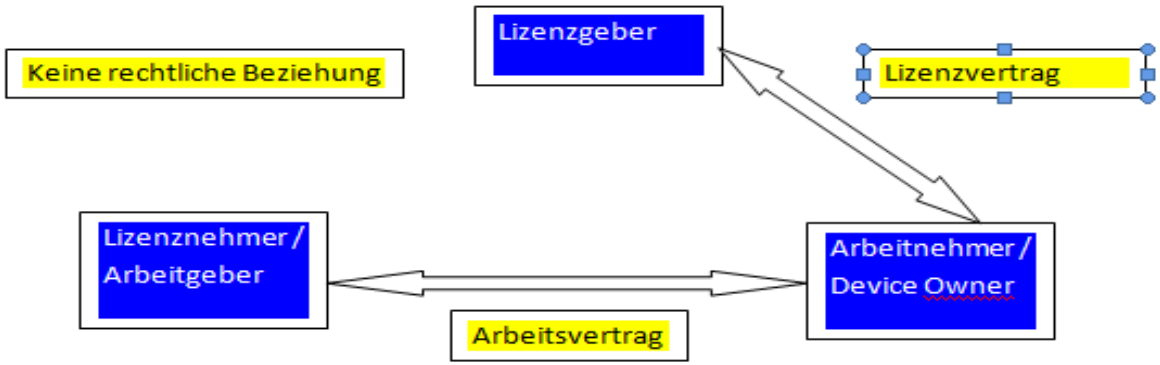
- Klassische Situation; der Arbeitgeber hat sicherzustellen, dass der Arbeitnehmer die Lizenzbestimmungen einhält.

Lizenzrechte BYOD Situation 1



- Es gilt vorab durch den Arbeitgeber als Lizenznehmer abzuklären, in wieweit eine Nutzung der Produkte durch den Arbeitnehmer auf seinem eigenen Device gemäss den Lizenzbestimmungen überhaupt zulässig ist.

Lizenzverträge BYOD Situation 2



- Der Arbeitnehmer hat den genauen Inhalt seiner Lizenzrechte vorab zu beachten und sicherzustellen, dass eine Nutzung zur Ausführung seiner Arbeit überhaupt zulässig ist.

Urheberrechtsverletzung

- **Zivilrechtlich** hat derjenige, der seine Rechte verletzt sieht zwei Möglichkeiten**:**
  - Art. 61 URG Feststellungsklage; er kann gerichtlich feststellen lassen ob er ein urheberrechtlich geschütztes Recht innehat.
  - Art. 62 URG Leistungsklage; er kann verlangen, dass eine drohende Verletzung verboten wird oder eine bestehende Verletzung beseitigt wird.
- Dem Beklagten /Verletzenden droht eine **Schadenersatzzahlung** und die Kosten für den Aufwand der gesetzeskonformen Zustand herzustellen.

Urheberrechtsverletzung

- **Strafrechtlich** wird eine Urheberrechtsverletzung wie folgt sanktioniert (Art. 67 Abs. 1 URG):
  - Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Vorausgesetzt der Verletzte hat einen Strafantrag gestellt (Antragsdelikt).
  - Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe in Fällen von gewerbsmässiger Urheberrechtsverletzung. Diese wird von Amtes wegen verfolgt (Art. 67 Abs. 2 URG).

Empfehlung

- Im Rahmen von BYOD verwendet der Mitarbeitende sein privates Device und allenfalls auch die darauf installierte Software (z.B. auf einem Notebook) für geschäftliche Zwecke.
- Lizenziert das Unternehmen die MDM-Software, die dann auf den privaten Devices des Mitarbeitenden installiert wird, stellt sich die Frage nach der Zulässigkeit dieses Vorgehens.
- In beiden Fällen sollten die lizenzrechtlichen Fragen geklärt werden, bevor BYOD gestattet wird!

Agenda

- Einführung in die rechtlichen Fragestellungen im Bereich Mobile Device Management
- Gesetzliche Anforderungen an die Datensicherheit
- Gesetzliche Anforderungen betreffend die Überwachung von Mitarbeitern
- Arbeitsrechtliche Aspekte
- Lizenzrechtliche Fragen
- **Mobile Device Management Policy**

MDM Policy – häufige Regelungen

- Welche Mitarbeitenden haben Anspruch auf ein geschäftliches MD?
- Welche Geräte (Hersteller, etc.) sind zulässig?
- Antragsverfahren, Bewilligung
- Übertragung von Rufnummern
- Möglichkeit, alte Geräte zu kaufen
- Vorgehen bei Ersatz von Geräten

Zwingend zu regeln

- Zulässigkeit / Verbot der privaten Verwendung geschäftlicher MD
- Zulässigkeit / Verbot von BYOD
- Sicherheitsvorgaben und Zuständigkeiten (Updates, Backups, Antivirenprogramme, etc.)
- Welche Daten dürfen die Mitarbeitenden mittels MD bearbeiten (Schutzklassen)?
- Überwachung des Geräts mittels MDM-Software
- Einwilligung des Mitarbeitenden bei BYOD
- Vorgehen bei Verlust des Geräts
- Rückgabe der MD bei Beendigung des Arbeitsverhältnisses
- Kosten

Überwachung regeln!

- In der Mobile Device Management Policy sollte klar geregelt werden
  - dass die Einhaltung der Policy überwacht wird
  - wie dabei vorgegangen wird
  - welche Folgen ein Verstoss haben kann.

Zusammenfassung

- Vor dem Einsatz von MD im Unternehmen sollten die damit zusammenhängenden Risiken geklärt werden.
- Sicherheitsvorgaben sowie die Frage der privaten Nutzung geschäftlicher Geräte und die geschäftliche Nutzung privater Devices (BYOD) sollten einheitlich und verbindlich geregelt werden.
- Im Zusammenhang mit BYOD entstehen zusätzliche regelungsbedürftige Probleme – dazu zählen insbesondere die Überwachung der Devices mittels MDM-Software und der Ersatz der Kosten.
- Allenfalls erforderliche **Einwilligungen** des Mitarbeitenden sollten vor der Gewährung des Zugriffs auf die geschäftlichen Daten bzw. die geschäftliche Infrastruktur eingeholt werden!

IT & LAW CONSULTING GMBH

Danke für die Aufmerksamkeit!

mag. iur. Maria Winkler

IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug

Telefon: +41 41 711 74 08
maria.winkler@itandlaw.ch