IT & LAW CONSULTING GMBH

Aus Mangel an Beweisen

Mit elektronischen Medien gerichtsfest archiviert und dokumentiert

mag. iur. Maria Winkler

SAQ Sektion Zentralschweiz

09. November 2012

Agenda

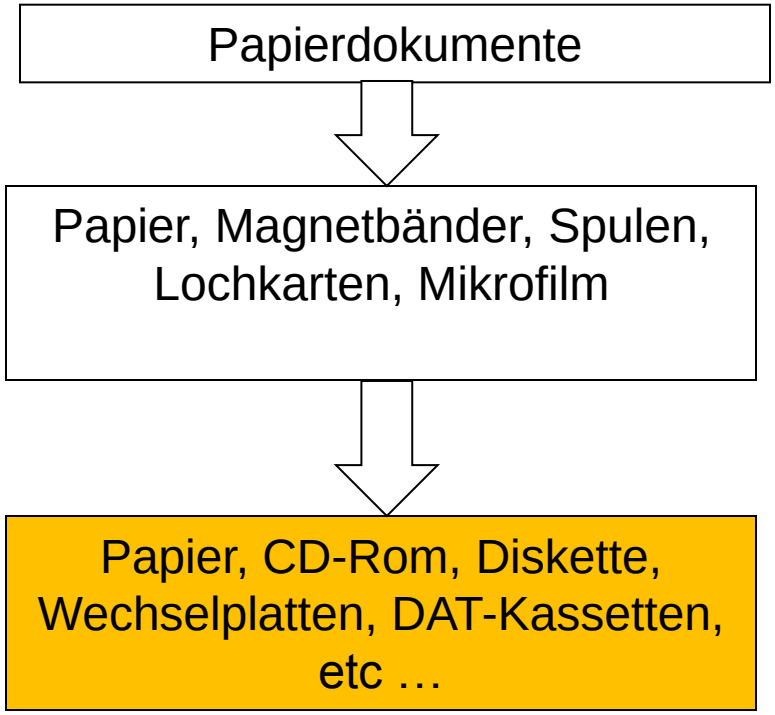
- Einführung
- Gesetzliche Grundlagen
- Aufbewahrungspflichtige Dokumente
- Anforderungen an die Aufbewahrung und Archivierung
- Datenschutzrechtliche Anforderungen an die Aufbewahrung und Löschung
- Elektronische Signatur: Funktionsweise und rechtliche Rahmenbedingungen

Die Archivierung im Wandel der Zeit

ursprünglich

seit ca. den 70er Jahren

heute



Dokumentenmanagement

- Der sorgfältige Umgang mit Geschäftsdokumenten umfasst die beiden folgenden Aufgabenbereiche:
  - **Identifikation** der für den eigenen Geschäftsbereich **relevanten Dokumente**.
  - Sicherstellung der **Integrität, Verfügbarkeit** und **Beweiskraft** dieser Dokumente über den gesamten Lebenszyklus.
- Um ein gesetzeskonformes Records Management sicherzustellen, müssen beide Aufgabenbereiche während des **ganzen Lebenszyklus** sorgfältig erfüllt werden.

Nachweis der Unternehmenstätigkeit

- Unternehmen müssen zum Nachweis der Unternehmenstätigkeit geschäftsrelevante Dokumente ablegen und archivieren.
- Geschäftsrelevant sind alle Dokumente, welche durch das Unternehmen **erstellt** werden oder welche dieses **von Dritten erhält** und welche
  - allgemein aus **Beweisgründen** zur Geltendmachung von eigenen Ansprüchen oder zur Abwehr von Ansprüchen Dritter benötigt werden;
  - sich in der **Buchhaltung** niederschlagen;
  - aufgrund besonderer **spezialgesetzlicher Vorschriften** erstellt und archiviert werden müssen;
  - das Unternehmen als **Gesellschaft betreffen** (Statuten, VR-Protokolle);
  - dem Nachweis der **Geschichte** des Unternehmens dienen.

Gesetzliche Grundlagen

- Gesetzesrevision im Gang
- Prozessrecht
- Steuerrecht (MWSTG, MWSTGV, ElDI-V)
- Archivgesetze (öffentlich-rechtlicher Bereich)
- Spezialgesetze (z.B. Produktehaftpflichtgesetz, Bankengesetz, etc.)

Kaufmännische Buchführung

- **Pflicht zur Buchführung** für **alle** juristischen Personen und Einzelunternehmen und Personengesellschaften mit einem Jahresumsatz über CHF 500‘000.-
  Pflicht zur einfachen Buchhaltung (Milchbüchleinrechnung) für Einzelunternehmen und Personengesellschaften mit einem Jahresumsatz unter CHF 500‘000.-, Vereine und Stiftungen die verpflichtet sind sich ins Handelsregister einzutragen sowie Stiftungen die von der Pflicht zur Bezeichnung der Revisionsstelle befreit sind. (=>Loslösung vom Grundsatz des Handelsregistereintrages)

Aufbewahrungspflichtige Dokumente

- Geschäftsbücher und Buchungsbelege (nicht mehr aber die Geschäftskorrespondenz) sowie Geschäfts- und Revisionsbericht
- Buchungsbelege sind alle für einen Geschäftsvorgang relevanten Belege (Inhalt, Betrag, Aussteller und Ausstelldatum müssen ersichtlich sein)
- Es muss nur jene Geschäftskorrespondenz aufbewahrt werden welche die Voraussetzung eines Beleges erfüllt.

E-Mail-Korrespondenz

- Wenn **E-Mails** geschäftsrelevante Informationen enthalten, unterliegen sie als Geschäftskorrespondenz ebenfalls der Aufbewahrungspflicht.
- **Achtung!** Gemäss der **Firmengebrauchspflicht** (Art. 954a OR) muss in der Korrespondenz, auf Bestellscheinen und Rechnungen sowie in Bekanntmachungen die im Handelsregister eingetragene Firma oder der im Handelsregister eingetragene Name vollständig und unverändert angegeben werden (in Kraft seit 01.01.2008).

Geschäftskorrespondenz und Buchungsbelege

Für Buchungsvorgang relevante Unterlagen	Ein- und ausgehende Briefe Verträge Telegramme, Fax, E-Mails Statuten und Gesellschaftsverträge Prozessakten, Gerichtsurteile, Vergleiche Dokumente aus Arbeitsverhältnissen, Dokumente aus Werkverträgen Dokumente aus dem Verkehr mit Behörden (Steuern und Sozialversicherungen)	buchungsrelevant
Buchungsbelege	Bank- und Postbelege Konto- Depotauszüge Lieferscheine Lohnabrechnungen Daten mit Belegcharakter Rechnungen und Quittungen Spesenabrechungen	

Aufbewahrung von E-Mails (Buchführung)

Zu archivierende E -Mails	Andere E -Mails
Bestellungen Auftragsbestätigungen Protokolle mit geschäftsrelevantem Inhalt Verträge Etc.	Offerten, welche nicht zum Vertragsabschluss führen (Ausnahme: Öffentlich-rechtlicher Bereich) Werbematerialien Anfragen Empfangsbestätigungen Preislisten

Policies und Weisungen

- Es liegt an den Unternehmen selbst, diese E-Mails zu identifizieren und zu archivieren.
- Durch den Erlass von **Weisungen und Policies** wird
  - bestimmt, welche Prozesse via E-Mail ablaufen dürfen
  - sichergestellt, dass alle geschäftsrelevanten E-Mails identifiziert werden
  - das Vorgehen betreffend der Archivierung festgelegt

Journaling

- Auf dem Markt sind zahlreiche Angebote für sogenannte „E-Mail-Archive“ erhältlich – dabei handelt es sich um Software und / oder Hardware, die eine integritätssichere Speicherung der E-Mails ermöglicht.
- Dabei werden alle ein- und ausgehenden E-Mails automatisch auf einem Datenträger gespeichert.
- **Achtung!** Die Archivierung von E-Mails ist nur dann gesetzeskonform, wenn sämtliche Voraussetzungen von Art. 957 ff OR sowie der GeBüV erfüllt sind.
- Da die E-Mail-Archive in der Regel z.B. keine Zuordnung der E-Mails zum Geschäftsfall ermöglichen, erfüllt das „Journaling“ in der Regel nicht sämtliche gesetzlichen Anforderungen.

E-Mail-Archivierung und Datenschutz

- In einer Weisung sollte geregelt werden, ob E-Mail privat genutzt werden darf.
- Bei **erlaubter privater Nutzung** ist die automatische Archivierung aller E-Mails ohne ausreichende Information der Mitarbeitenden **unzulässig**! Den Mitarbeitenden sollte zudem die Möglichkeit geboten werden, private E-Mails der automatischen Archivierung zu entziehen.
- Bei **privater Nutzung untersagt**, dann dürfen alle E-Mails automatisch archiviert werden. Der Arbeitgeber darf aber (gegen die Weisung verstossende) private E-Mails dennoch nicht öffnen und lesen!

Dasselbe findet für E-Mails, welche als belegrelevant gelten, Anwendung.

Archivierungsfrist

- Die **handelsrechtliche Archivierungsfrist** beträgt **10 Jahre**. Da diese erst mit dem Ende des Geschäftsjahres beginnt, beträgt die gesamte Aufbewahrungs- und Archivierungsdauer der Dokumente bis zu 11 Jahre.
- Die **steuerrechtliche Archivierungsfrist** beträgt in der Regel ebenfalls **10 Jahre**. Gemäss MWSTG müssen aber Belege im Zusammenhang mit Liegenschaften **20 Jahre** archiviert werden.

Verjährungsfristen

- Grundsätzlich ist zu beachten, dass die **Verjährung einer Forderung** (z.B. bei Dauerschuldverhältnissen) oft nicht bereits mit dem Ende des Geschäftsjahres, sondern zu einem späteren Zeitpunkt beginnt, wodurch sich die Aufbewahrungs- und Archivierungsdauer ebenfalls verlängert.

Schriftlich oder elektronisch?

- - Buchungsbelege und Geschäftsbücher: auf Papier, elektronisch oder in vergleichbarer Weise (Art. 9 GebüV).
- - Geschäfts- und Revisionsbericht: Im Moment herrscht diesbezüglich noch keine Klarheit. Empfehlung: Papierform oder Papierform kombiniert mit einer anderen Aufbewahrungsweise.

und aufbewahrt werden

- wenn die Übereinstimmung mit den zugrunde liegenden Geschäftsfällen gewährleistet ist und
- sie jederzeit lesbar gemacht werden können.

Aufbewahrungsform

Aufbewahrungsform / Dokument	Schriftlich und unterzeichnet	Schriftlich, elektronisch oder in vergleichbarer Form
Bilanz und Betriebsrechnung	X	
Geschäftsbücher		X
Buchungsbelege		X
Geschäftskorrespondenz		X

Spezialgesetze

- Die Vorschriften der kaufmännischen Buchführung haben das Ziel, das Finanzgebaren des Unternehmens überprüfbar zu machen und so die Interessen von Gläubigern zu schützen
- Zahlreiche Branchen unterliegen zudem **spezialgesetzlichen Vorschriften**, welche direkt oder indirekt eine Pflicht zur Erstellung und Aufbewahrung von Dokumenten enthalten
- Im Folgenden werden Beispiele aus dem **privatrechtlichen Bereich** besprochen

Produktehaftpflichtgesetz (PrHG)

Art. 5 PrHG

1 Die Herstellerin **haftet nicht**, **wenn sie beweist**, dass:

a. sie das Produkt nicht in Verkehr gebracht hat;

b. nach den Umständen davon auszugehen ist, dass der Fehler, der den Schaden verursacht hat, noch nicht vorlag, als sie das Produkt in Verkehr brachte;

c. sie das Produkt weder für den Verkauf oder eine andere Form des Vertriebs mit wirtschaftlichem Zweck hergestellt noch im Rahmen ihrer beruflichen Tätigkeit hergestellt oder vertrieben hat;

d. der Fehler darauf zurückzuführen ist, dass das Produkt verbindlichen, hoheitlich erlassenen Vorschriften entspricht;

e. der Fehler nach dem Stand der Wissenschaft und Technik im Zeitpunkt, in dem das Produkt in Verkehr gebracht wurde, nicht erkannt werden konnte.

Produktehaftpflichtgesetz (PrHG)

Die Herstellerin eines Grundstoffs oder eines Teilprodukts haftet ferner nicht, wenn sie beweist, dass der Fehler durch die Konstruktion des Produkts, in das der Grundstoff oder das Teilprodukt eingearbeitet wurde, oder durch die Anleitungen der Herstellerin dieses Produkts verursacht worden ist.

Art. 10 PrHG

Die Ansprüche aus dem PrHG **verwirken 10 Jahre ab dem Tag**, an dem die Herstellerin das Produkt, das den Schaden verursacht hat, **in Verkehr gebracht** hat.

- Insbesondere bei der Herstellung von Serienprodukten ist zu beachten, dass die Aufbewahrungsfrist viel länger als 10 Jahre sein kann, da meist nicht nachgewiesen werden kann, wann das einzelne Produkt genau in Verkehr gebracht wurde und man daher die entsprechenden Unterlagen ab dem Zeitpunkt archivieren sollte, in dem das letzte Produkt der Serie im Verkehr gebracht wurde.

Informationspflichten börsennotierter Unternehmen

- Art. 53 des **Kotierungsreglements der SIX** regelt die Pflicht on börsennotierten Unternehmen, börsenrelevante Informationen, welche den Kurs der Effekte beeinflussen können, möglichst zeitnah zu publizieren (Ad-hoc-Publizität).
- Gemäss der **Richtlinie über die Ad hoc-Publizität** sind **Ad-hoc Mitteilungen** zumindest an folgende Adressaten zu verbreiten:
  - SIX Swiss Exchange (90 Minuten im Voraus, falls während der Handelszeit publiziert)
  - Mindestens zwei bei professionellen Marktteilnehmern verbreitete elektronische Informationssysteme (z.B. Bloomberg, Reuters, SIX Telekurs)
  - Mindestens zwei Schweizer Zeitungen von nationaler Bedeutung
  - Jedem Interessierten auf Anfrage (Push- und Pullsystem)

Push- und Pull-System

- Der Emittent stellt auf seiner Website einen Dienst zur Verfügung, welcher es Interessierten ermöglicht, über einen **E-Mail-Verteiler** kostenlos und zeitnah potentiell kursrelevante Tatsachen zugesandt zu erhalten (**Push-System**).
- Jede publizierte Ad hoc-Mitteilung ist zeitgleich mit der Verbreitung **auch auf der Website des Emittenten** aufzuschalten und muss dort während zwei Jahren abrufbar sein (**Pull-System**).
- Quelle: Website der SIX (: unter http://www.six-exchange-regulation.com/admission_manual/06_16-DAH_de.pdf)
- Die Verletzung dieser Pflichten wird von der SIX sanktioniert. Börsennotierte Unternehmen sollten daher den **Inhalt ihrer Websites** jederzeit nachweisen können!

FINMA-Rundschreiben

- Das Rundschreiben 08/38 enthält **Aufsichtsregeln zum Marktverhalten im Effektenhandel**
- Es gilt für Banken, Effektenhändler, Vermögensverwalter, etc.
- Verlangt wird z.B. die Aufzeichnung aller Effektengeschäfte, aber auch die Aufzeichnung der **Telefongespräche** der Mitarbeitenden sowie von deren **E-Mails**
- Telefongespräche und E-Mails müssen der FINMA für **6 Monate** zu Untersuchungszwecken **unverändert** zugänglich gemacht werden

Fazit

- Jedes Unternehmen muss die jeweils für den **eigenen Geschäftsbereich** vorgeschriebenen aufbewahrungs-pflichtigen Dokumente identifizieren.
- Bei der Festlegung der Archivierungsfrist sind neben den gesetzlichen Grundlagen der Art. 957 ff. OR auch Verjährungsfristen sowie die Anforderungen von branchenspezifischen Gesetzen zu berücksichtigen.
- Der Umgang mit aufbewahrungspflichtigen Dokumenten sollte in Policies verbindlich geregelt werden.

Beweiskraft

- Gemäss Art. 178 ZPO hat die Partei, die sich auf eine Urkunde beruft, die **Echtheit** zu beweisen, sofern diese von der anderen Partei bestritten wird. Bei der Beweisführung muss in der Regel nachgewiesen werden, dass die Voraussetzungen der **Geschäftsbücherverordnung (GeBüV)** erfüllt sind.
- Art. 3 GeBüV verlangt, dass die Geschäftsdokumente so **geführt und aufbewahrt** werden, dass sich **nachträgliche Änderungen** feststellen lassen.
- Um die **Beweiskraft** der Dokumente zu sichern, muss deren Integrität bereits **nach Fertigstellung oder Eingang** gesichert werden und nicht erst bei der Archivierung.

Integritätssicherung bei der Archivierung

- Zur Integritätssicherung können unterschiedliche **technische und/oder organisatorische Massnahmen** wie z.B. Signaturen, unveränderbare Datenträger, Verschlüsselungen, die restriktive Erteilung von Zugriffsberechtigungen, die Aufzeichnung von Zugriffen, etc. verwendet werden.
- Die Speicherung auf veränderbaren Datenträgern ist erlaubt,
  - wenn technische Verfahren Integrität gewährleisten (z.B. digitale Signatur)
  - und der Zeitpunkt der Speicherung nachweisbar ist (Zeitstempel)
  - und die Abläufe, Verfahren und Hilfsinformationen protokolliert werden.

Dokumentationspflichten

- Umfangreiche Dokumentationspflichten stellen sicher, dass die Geschäftsbücher, Buchungsbelege und die Geschäftskorrespondenz während der gesamten Aufbewahrungsdauer **verstanden** werden können
- Die Dokumentationen sind **aktuell** zu halten und müssen gleich lang aufbewahrt werden, wie die Geschäftsbücher.

Verfügbarkeit

- Die aufbewahrten Dokumente müssen innerhalb einer **angemessenen Frist** von **berechtigten Personen** eingesehen und überprüft werden können.
- Personal, Geräte und Hilfsmittel sind während der gesamten Aufbewahrungsdauer zur Verfügung zu halten!
- Die Dokumente müssen auch in Papierform vorgelegt werden können.

Organisation

- Archivierte Dokumente müssen von aktiven Informationen **getrennt** oder so gekennzeichnet werden, dass eine Unterscheidung möglich ist.
- Der **Zugriff** auf die archivierten Dokumente muss geregelt werden, Zugriffe und Zutritte sind aufzuzeichnen.
- Die archivierten Dokumente müssen regelmässig auf ihre **Lesbarkeit** überprüft werden.
- Eine **Migration** auf andere Formate oder andere Datenträger zur Gewährleistung der Lesbarkeit ist erlaubt. Der Vorgang der Migration muss protokolliert und die Protokolle müssen archiviert werden.

Scannen von Papierbelegen

- Das Scannen und die anschliessende elektronische Ablage und Archivierung von Papierdokumenten (Verträge, Kreditorenrechnungen) ist erlaubt, wenn sichergestellt wird, dass
  - die **Vollständigkeit** und **Richtigkeit** der Information gewährleistet bleibt und
  - die **Verfügbarkeit** und die **Lesbarkeit** den gesetzlichen Anforderungen weiterhin genügen.
- Der Scanprozess stellt eine Migration auf einen anderen Datenträger gemäss Art. 10 GeBüV dar.
- Der Scanprozess muss protokolliert und das **Protokoll** muss mit archiviert werden. Dabei müssen die verwendete technische Infrastruktur beschrieben und die Arbeitsanweisungen dokumentiert werden (**Verfahrensdokumentation**).

Scanprozess

- Es ist sicherzustellen, dass **alle Belege eingescannt** werden und die gewonnene **Datei auch tatsächlich lesbar ist**.
- Es dürfen nur **Belege vernichtet** werden, die **korrekt eingescannt** wurden.
- Die **Integrität** der Dokumente muss vom Eingang über den Zeitpunkt des Einscannens bis zu ihrer Vernichtung sichergestellt werden.
- Das eingescannte Dokument muss unmittelbar nach dem Scann-Vorgang z.B. mittels Signatur **vor Veränderungen geschützt** werden.
- Die **Einsicht und Prüfung** innerhalb einer angemessenen Frist müssen möglich sein.
- **Nur wenn die gesetzlichen Voraussetzungen erfüllt sind, darf der Papierbeleg nach dem Scannen vernichtet werden!**

Beweiskraft des elektronischen Belegs

- Gemäss einer Stellungnahme des Eidgenössischen Finanzdepartementes ist **die Vernichtung des Originalbeleges** unter Beachtung der gesetzlichen Vorgaben zwar **erlaubt**. Es sei aber zu beachten, dass dem Steuerpflichtigen dadurch durchaus auch **Nachteile** entstehen können.
- Das Originaldokument sei immer aussagekräftiger als seine elektronische Aufzeichnung. Durch die Vernichtung des Originaldokuments werde das **faktische Problem** geschaffen, dass es nicht mehr möglich sei, Sachverhalte, welche nur anhand des Originaldokuments festgestellt werden können, zu überprüfen. Auch die Überprüfung, ob der Inhalt des Belegs vollständig und richtig übertragen wurde, ist nachträglich nicht mehr möglich.

Der elektronische Beleg in der MWST

- Die Steuerbehörden akzeptieren für die Berechnung der Mehrwertsteuer und für die Geltendmachung des Vorsteuerabzugs neben Papierbelegen auch die folgenden elektronischen Belege:
  - elektronische Kopien von **eingescannten Papierbelegen**, wenn diese nach den Vorschriften der GeBüV archiviert wurden;
  - **elektronische Kopien** von **in Papierform versandten Ausgangsrechnungen**, wobei nicht erforderlich ist, dass diese vorher ausgedruckt und gescannt werden, sofern diese nach den Vorschriften der GeBüV archiviert werden;
  - **elektronische Ursprungsbelege**, wenn diese nach den Vorschriften der ElDI-V übermittelt und aufbewahrt wurden (Verordnung des EFD vom 30.01.2002 über elektronische Daten und Informationen).

Elektronische Rechnungsstellung

- Im Rahmen des **E-Billings** müssen der **Ursprung**, die **Integrität** sowie der **Versand und der Empfang** nachgewiesen werden können.
  - Die Übermittlung und Aufbewahrung müssen mittels **digitaler Signatur** abgesichert sein.
  - Es muss ein **Zertifikat** eines anerkannten Anbieters von Zertifizierungsdiensten verwendet werden, das im Zeitpunkt der Signaturerstellung **gültig** ist.
  - Die Daten müssen bei einer automatisierten Verarbeitung vor ihrer Verwendung **verifiziert** und das Ergebnis muss **protokolliert** werden.
  - Der öffentlichen Schlüssel muss aufbewahrt werden und es müssen **sichere Signaturen** verwendet werden.
  - Bei Einsatz von Kryptographie muss der Schlüssel zur **Entschlüsselung** aufbewahrt werden.

Verantwortung

- Der VR ist verantwortlich für die **Oberleitung der Gesellschaft** und für die Erteilung der nötigen Weisungen.
- Er muss die **Einhaltung von Gesetzen und Weisungen** überprüfen und ist verantwortlich für die Ausgestaltung des **Rechnungswesens und der Finanzkontrolle**.
- Er kann diese Pflichten nicht delegieren und haftet für deren Verletzung (Art. 754 OR).
- Der VR ist daher zuständig für die Regelung von Verantwortlichkeiten, den Erlass von **Weisungen** und deren Kontrolle, die Bereitstellung der erforderlichen Infrastruktur sowie der personellen und finanziellen **Ressourcen**.

Schlussbemerkungen

- Die Definition von Vorgaben über den Umgang mit Geschäftsdokumenten ist **Chefsache**.
- Dabei muss die **Verfügbarkeit** und **Integrität** der Dokumente über den ganzen Lebenszyklus von deren Entstehung über die Aufbewahrung bis zur Vernichtung sichergestellt werden.
- Neben den Buchführungsvorschriften und den steuerrechtlichen Vorgaben muss auch den Anforderungen von Spezialgesetzen, des Datenschutzes sowie von Geheimhaltungspflichten genügend Beachtung geschenkt werden.

Agenda

- Einführung
- Gesetzliche Grundlagen
- Aufbewahrungspflichtige Dokumente
- Anforderungen an die Aufbewahrung und Archivierung
- **Datenschutzrechtliche Anforderungen an die Aufbewahrung und Löschung**
- Elektronische Signatur: Funktionsweise und rechtliche Rahmenbedingungen

Datenschutz

Datenschutzgesetz Bund (seit 1993)

Datenbearbeitung durch

- Bundesbehörde
- Private
- Teilrevision auf 01.01.2008 in Kraft getreten

Kantonale Datenschutz-gesetzgebungen

Datenbearbeitung durch

- kantonale und
- kommunale Behörden

Personendaten

- **Personendaten**
  Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen
- **Besonders schützenswerte Personendaten**
  Angaben über:
  - religiöse, weltanschauliche oder politische Haltung
  - Intimsphäre, Gesundheit, ethnische Zugehörigkeit
  - Massnahmen der Sozialhilfe
  - administrative und strafrechtliche Massnahmen und Sanktionen

Persönlichkeitsprofile

- **Persönlichkeitsprofile** sind eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person erlaubt
- Personalakten können z.B. ein Persönlichkeitsprofil darstellen
- Bei **besonders schützenswerten Personendaten** und **Persönlichkeitsprofilen** besteht eine besonders grosse Gefahr der Persönlichkeitsverletzung –ihre Bearbeitung muss daher besonders sorgfältig erfolgen

Verhältnismässigkeit (Art. 4 Abs. 2 DSG)

- **Verhältnismässigkeit**
  - Bearbeitung nur soweit wie für Aufgabenerfüllung notwendig und geeignet
  - Beschränkung auf das Notwendige und tatsächlich Erforderliche
  - Keine Datensammlung auf Vorrat
- **Umsetzung**
  - Beschränkung der Zugriffsrechte (need to know)
  - Es dürfen nur so viele Daten bearbeitet werden, wie für die Erreichung des beabsichtigten Zwecks erforderlich sind
  - Nicht mehr benötigte Daten müssen **vernichtet** oder anonymisiert/ pseudonymisiert werden, sofern keine Archivierungs- oder Aufbewahrungspflicht bestehen

Datensicherheit (Art. 7 DSG)

- Personendaten müssen durch **angemessene technische und organisatorische Massnahmen** gegen unbefugtes Bearbeiten, gegen die zufällige oder absichtliche Vernichtung, etc. geschützt werden.
- Die **Angemessenheit** der Massnahmen hängt von der Sensibilität der Daten ab – je grösser die Gefahr der Persönlichkeitsverletzung, umso höher ist die Sorgfaltspflicht beim Schutz der Daten.
- Diese Vorgaben sind auch bei der Aufbewahrung und **Vernichtung** der Daten zu beachten!

Vernichtung von Daten und Dokumenten

- Nach Ablauf der gesetzlichen oder betrieblichen Archivierungsfrist dürfen **private Unternehmen** die Geschäftsdokumente vernichten.
- Werden **Personendaten** (z.B. Personal- oder Patientendossiers, Kundendossiers) ohne Rechtfertigungsgrund länger archiviert als gesetzlich vorgesehen, dann stellt dies eine **unverhältnismässige Datenbearbeitung** dar.
- **Öffentlich-rechtliche Institutionen** müssen die Akten dem Staats- oder Bundesarchiv anbieten - übernimmt dieses die Akten nicht, dann **müssen** diese vernichtet werden (z.B. Art. 21 Abs. 2 DSG).
- Dabei sind **datenschutzrechtliche Grundsätze** zu beachten!

Zwischenfazit

- Eine **Pflicht zur Vernichtung von Personendaten** besteht ausdrücklich im öffentlich-rechtlichen Bereich, wenn die Daten nicht vom zuständigen Archiv übernommen werden.
- **Private Unternehmen** müssen Dokumente, welche Personendaten enthalten, nach dem Grundsatz der Verhältnismässigkeit dann vernichten, wenn sie diese nicht mehr benötigen und sie diese auch nicht mehr archivieren müssen.
- Eine Pflicht zur Vernichtung von Dokumenten kann sich auch aus einer gesetzlichen oder vertraglichen **Geheimhaltungspflicht** ergeben!

Datenschutzkonforme Vernichtung

- Besteht eine **grosse Gefahr der Verletzung von Persönlichkeitsrechten**, oder besteht eine gesetzliche oder vertragliche **Geheimhaltungspflicht**, dann muss die Vernichtung besonders sorgfältig erfolgen.
  - Elektronische Daten müssen so gelöscht werden, dass sie nicht wieder hergestellt werden können
  - Ist dies nicht möglich, dann muss der Datenträger zerstört werden
  - Papierdokumente müssen geshreddert werden
  - Die Vernichtung durch Dritte muss kontrolliert erfolgen
- Es ist bei der anzuwendenden Sorgfalt abzustellen auf den **aktuellen Stand der Technik**!

Probleme in der Praxis

- **Wartungsverträge** mit Hardware-Lieferanten sehen oft vor, dass kaputte Datenträger zurückgesandt werden müssen – diese werden dann repariert und wieder verkauft. Es muss in diesem Fall **vertraglich sichergestellt** werden, dass die sich auf dem Datenträger befindlichen Informationen definitiv gelöscht werden – es empfiehlt sich, hier eine Konventionalstrafe zu vereinbaren, falls dagegen verstossen wird.
- **Mitarbeitende** müssen sensibilisiert werden, wie Daten und Dokumente richtig gelöscht bzw. vernichtet werden – zudem sind die Mittel zur korrekten Erfüllung dieser Pflicht zur Verfügung zu stellen.

Verantwortung

- Der VR und die GL sind zuständig für die Regelung von Verantwortlichkeiten, den Erlass von **Weisungen** und deren Kontrolle, die Bereitstellung der erforderlichen Infrastruktur sowie der personellen und finanziellen **Ressourcen**. Sie müssen zudem sicherstellen, dass die Mitarbeitenden geschult werden.
- Die **Mitarbeitenden** sind verpflichtet, Weisungen zu beachten und haben zudem eine Treuepflicht gegenüber dem Arbeitgeber. Der Arbeitgeber kann bei einer Verletzung der Weisungen Schadenersatz verlangen.
- Werden **strafrechtliche Bestimmungen** verletzt, dann ist die tatsächlich verantwortliche natürliche Person strafbar!

Agenda

- Einführung
- Gesetzliche Grundlagen
- Aufbewahrungspflichtige Dokumente
- Anforderungen an die Aufbewahrung und Archivierung
- Datenschutzrechtliche Anforderungen an die Aufbewahrung und Löschung
- **Elektronische Signatur: Funktionsweise und rechtliche Rahmenbedingungen**

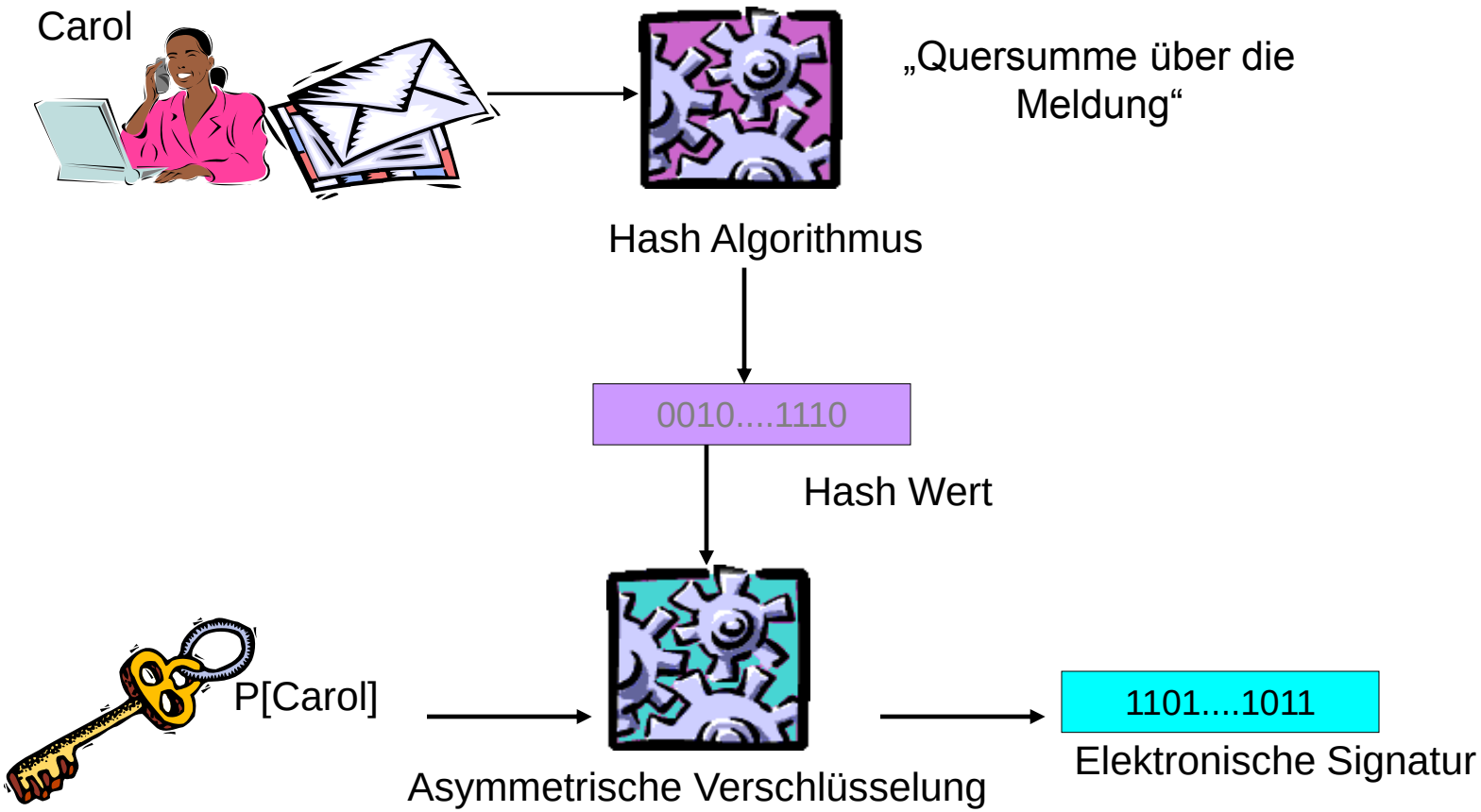
Elektronische Signatur – warum?

- Die elektronische Signatur kann eingesetzt werden, um
  - Erklärungen, welche der **Schriftform** bedürfen, auch elektronisch rechtsverbindlich abzugeben und
  - um die **Beweiskraft** von Dokumenten und Prozessen zu erhöhen.

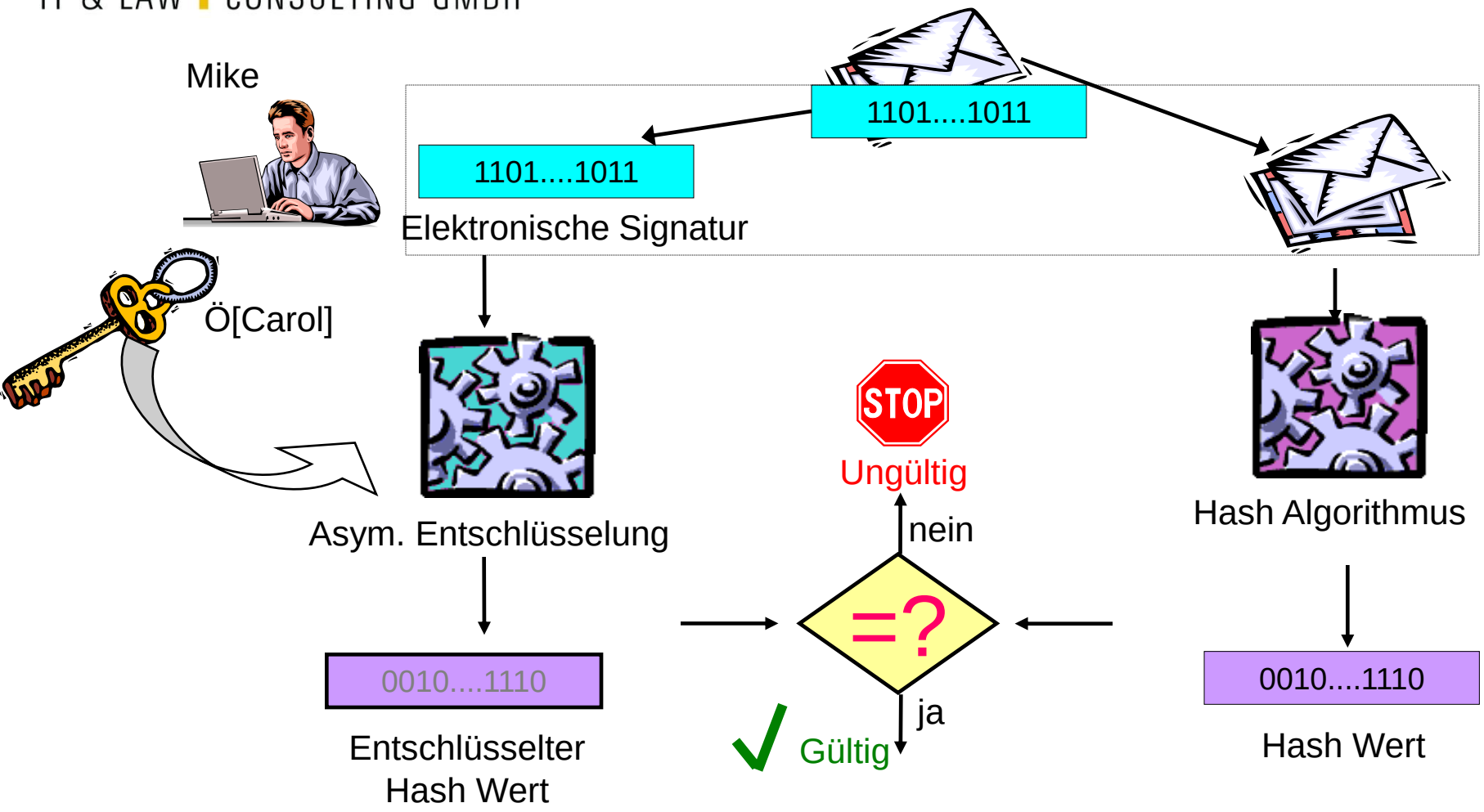
Funktionsweise

- Bei der elektronischen Signatur handelt es sich um ein kryptografisches Verfahren, welches mit zwei asymmetrischen Schlüsseln arbeitet
  - Mit dem **privaten, geheim zu haltenden Schlüssel** wird der Hashwert des Dokuments (= „Komprimat des Textes, bestehend aus einer Abfolge der Zahlen 0 und 1) **verschlüsselt**
  - Der **öffentliche Schlüssel** kann nur zur **Entschlüsselung** verwendet werden und passt nur zu einem bestimmten privaten Schlüssel; er kann öffentlich bezogen werden und wird häufig mit der Nachricht mit gesandt

Prinzip der Public Key Verfahren
Elektronische Signatur



Prinzip der Public Key Verfahren
Elektronische Signatur



Zertifikate

- Die Zuordnung der elektronischen Signatur zum Inhaber erfolgt mittels Zertifikaten
- Es handelt sich dabei um eine **elektronische Bescheinigung**, welche den öffentlichen Signaturprüfschlüssel mit dem Namen des Inhabers verknüpft (natürliche oder juristische Person)

Gesetzliche Grundlagen

- Die folgenden Normen regeln die **Anerkennung der Anbieterinnen von Zertifizierungsdiensten**
  - Bundesgesetz über die Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES; befindet sich in Revision)
  - Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES)
  - Technische und administrative Vorschriften (TAV)
- Zusätzlich trat mit dem Erlass des ZertES **Art. 14 Abs. 2bis OR** in Kraft, der die Voraussetzungen für Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift regelt

Arten von Signaturen nach ZertES

- **Elektronische Signatur**
  - Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen
- **Fortgeschrittene elektronische Signatur**
- **Qualifizierte elektronische Signatur**
- Mit der Revision des ZertES soll eine sogenannte **„geregelte elektronische Signatur“** für natürliche und juristische Personen sowie für Behörden eingeführt werden. Sie bildet einen Spezialfall der fortgeschrittenen elektronischen Signatur. Die Vernehmlassungsfrist ist Ende Juni 2012 abgelaufen.

Fortgeschrittene elektronische Signatur

Elektronische Signatur, die

- ausschliesslich der Inhaberin oder dem Inhaber zugeordnet ist
- die Identifizierung des Inhabers oder der Inhaberin ermöglicht
- mit Mitteln erzeugt wird, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann
- mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass eine nachträgliche Veränderung erkannt werden kann

Anwendungsbereich

- Der **Inhaber** einer fortgeschrittenen elektronischen Signatur kann auch ein Unternehmen, ein Server, eine Applikation, etc. sein
- Die fortgeschrittene elektronische Signatur kann daher zum **Signieren von Dokumenten** verwendet werden, wenn **keine** gesetzlichen **Formvorschriften** bestehen (persönliche Zertifikate)
- Mit der fortgeschrittenen elektronischen Signatur sind **Massensignaturen** möglich - sie dient der **Integritätssicherung** von Dokumenten im Bereich der elektronischen Rechnungsstellung oder der Archivierung (Funktionszertifikate)

Qualifizierte elektronische Signatur

- Eine fortgeschrittene elektronische Signatur, welche auf einer sicheren Signaturerstellungseinheit und auf einem qualifizierten und zum Zeitpunkt der Erzeugung gültigen Zertifikat beruht.

Qualifiziertes Zertifikat

- Seriennummer
- Hinweis auf qualifiziertes Zertifikat
- Name des Inhabers (**natürliche Person**)
- Signaturprüfschlüssel
- Gültigkeitsdauer
- Zertifizierungsdienststelle
- Nutzungsbeschränkungen

Gleichstellung mit der Handunterschrift

- Ein Vertrag, für den die schriftliche Form gesetzlich vorgeschrieben ist, muss die Unterschriften aller Personen tragen, die durch ihn verpflichtet werden (Art. 13 Abs. 1 OR).
- Die Unterschrift ist eigenhändig zu schreiben (Art. 14 Abs. 1 OR).
- Der eigenhändigen Unterschrift gleichgestellt ist die **qualifizierte elektronische Signatur**, die auf einem qualifizierten Zertifikat einer **anerkannten Anbieterin** von Zertifizierungsdiensten im Sinne des ZertES beruht (Art. 14 Abs. 2 bis OR).

Schriftlichkeit

- Schriftlichkeit im Privatrecht wird beispielsweise in den folgenden Fällen verlangt:
  - **Abtretung** einer Forderung (Art. 165 OR)
  - **Konsumkreditvertrag** (Barkreditvertrag; Leasingvertrag, wenn dieser vorsieht, dass die Leasingrate erhöht wird, falls der Vertrag vorzeitig aufgelöst wird; Kredit- und Kundenkarten, wenn eine Ratenzahlung möglich ist)
  - **Nachvertragliches Konkurrenzverbot** im Arbeitsvertrag (Art. 340 OR)
  - Wenn die Vertragsparteien diese **vereinbaren** (Art. 16 OR)
- Für die meisten Verträge, welche über das Internet abgeschlossen werden, bestehen **keine Formvorschriften** (z.B. Kaufverträge, Lizenzverträge, Aufträge, Werkverträge, etc.)

Anbieterin von Zertifizierungsdiensten

- Die Anbieterin von Zertifizierungsdiensten bestätigt als vertrauenswürdige Dritte, dass ein öffentlicher Prüfschlüssel einer bestimmten natürlichen Person zugeordnet werden kann
- Die Anbieterin ist verpflichtet, die **Identität** des Antragsstellers zu überprüfen
- Anerkannte Anbieterinnen nach ZertES
  - Swisscom Schweiz AG
  - QuoVadis Trustlink Schweiz AG
  - Swiss Sign (100% - Tochter der Post)
  - Bundesamt für Informatik und Telekommunikation BIT

Beweiskraft elektronischer Urkunden

- Elektronische Dokumente müssen unter Umständen einem Gericht oder einer Behörde als Beweismittel vorgelegt werden
- Wird die **Beweiskraft** des elektronischen Dokumentes angezweifelt, dann scheitert u.U. die Beweisführung!
- Die Verwendung der elektronischen Signatur erhöht die **Beweiskraft** der elektronisch ausgetauschten geschäftsrelevanten Dokumente.

Erhöhung der Beweiskraft

- **Elektronische Signaturen** ermöglichen den Nachweis der Identität der signierenden Person und den Nachweis, dass das Dokument nicht verändert wurde.
- Elektronische Signaturen ermöglichen jedoch **nicht** den Nachweis, dass ein elektronisches Dokument **versandt** oder **empfangen** wurde
- Elektronische Signaturen ermöglichen zudem **nicht** den Nachweis, **was** am ursprünglichen Dokument **geändert** wurde!

Einsatzbereiche der elektronischen Signatur

- **Ersatz für Handunterschrift (Rechtsverbindlichkeit)**
  - Schreibt das Gesetz die Schriftform vor, dann muss im elektronischen Geschäftsverkehr die elektronische Signatur gemäss Art. 14 Abs. 2 bis OR verwendet werden
- **Integritätssicherung**
  - Mit digitalen Signaturen kann nachgewiesen werden, ob ein Dokument nach dem Zeitpunkt des Signierens noch geändert wurde
- **Authentizität**
  - Mit digitalen Signaturen kann die (natürliche oder juristische) Person, welche das Dokument signiert hat, identifiziert werden
- **Autorisierung**
  - Rechte und Befugnisse des Signierenden können in den Zertifikaten angegeben und damit verwaltet werden

Welche Signatur wofür?

- Je nachdem, welcher Zweck erreicht werden soll, müssen einfache, fortgeschrittene oder qualifizierte elektronische Signaturen verwendet werden
- **Qualifizierte Signaturen** (gemäss Art. 14 Abs. 2 bis OR) müssen verwendet werden, wenn das Gesetz im „normalen Geschäftsverkehr“ die Handunterschrift verlangt
- **Fortgeschrittene Signaturen** dienen in erster Linie der Integritätssicherung

Suisse ID

- Elektronische Identitäten sind die Voraussetzung für die sichere Kommunikation in der Privatwirtschaft und im eGovernment
- Seit Mai 2010 ist die **SuisseID** erhältlich – es handelt sich um ein elektronisches Zertifikat auf Smartcard oder USB Token inkl. Funktionsregister (qualifiziertes und fortgeschrittenes Zertifikat mit Funktionsregister)
- Herausgeber sind die anerkannten Anbieterinnen von Zertifizierungsdiensten.

Schlussbemerkung

- Elektronische Signaturen unterstützen dabei, elektronische Prozesse sicherer zu machen
- Um die für den geplanten Zweck geeignete elektronische Signatur zu finden, müssen gesetzliche Anforderungen und technisch/organisatorische Rahmenbedingungen berücksichtigt werden
- Zudem muss beachtet werden, dass für die Gewährleistung der Vertraulichkeit zusätzliche Verschlüsselungsmassnahmen getroffen werden müssen
- Wann und in welcher Form die revidierten Bestimmungen der ZertES in Kraft treten werden, ist noch ungewiss.

IT & LAW CONSULTING GMBH

Haben Sie Fragen ?

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Grafenaustrasse 5
6300 Zug

Tel: +41 41 711 74 08

maria.winkler@itandlaw.ch

Publikationen

www.itandlaw.ch