Rechtliche Aspekte zum Records-Managements

Rechtliche Aspekte zum Records-Managements & Langzeitarchivierung

Teil 1: Governance und Sorgfaltspflichten ausgewählte Rechtsaspekte

- Gesetzliche Vorgaben
- Normen, Standards und Richtlinien
- Aufbewahrungspflichten
- Urkundenqualität digitaler Akten
- Elektronische Signaturen und E-ID

Teil 2: Die Bedeutung von Records im Rechtsstreit

- Einsatz elektronischer Signaturen
- Beweiswert nachträglich eingescannter Akten

Praktische Übung (RM-Policy erarbeiten)

Lukas Fässler Rechtsanwalt

Rechtsanwalt und Informatikexperte,
Certified Software Asset Manager IAITAM Inc.

Profil

1975 – 1980	Studium an der Universität Fribourg/CH
1982	Anwaltspatent des Kantons Luzern
1982 – 1984	Gerichtsschreiber am Amtsgericht Hochdorf
1984 - 1987	Gerichtsschreiber am Verwaltungsgericht Luzern
1987 - 1992	EDV-Beauftragter im Gerichtswesen Kanton Luzern
1992 - 1997	Informatikchef des Kantons Luzern
1997	Selbständiger Spezialanwalt seit September 1997
1999 - 2000	Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht)
2017	"Certified Software Asset Manager IAITAM Inc." bei der International Association of Information Techology Asset Managers Inc. in Amerika

VRP AR Informatik AG	(2019 ff.)
Vizepräsident VR ILZ OW/NW	(2001 ff.)
Vizepräsident VR HIN AG	(2000 ff.)
Präsident Verein SSGI	(2005 ff.)
VRP Viacar AG	(2010-2012)
Dozent Fachhochschule NW in Basel	
Dozent Universität Basel	
Dozent Universität Bern/Lausanne	

Alle nachfolgenden Ausführungen gelten im Grundsatz analog sowohl für

- **Öffentlich-rechtliche Körperschaften**
  - Verwaltungen von Bund, Kantonen, Gemeinden
  - Exekutiven (Regierungsrat, Stadtrat)
  - Gerichte (Bundesgericht, Kantonsgerichte, Bezirksgerichte)
- **Private Unternehmen**
  - Personengesellschaften (Vereine, einfache Gesellschaften, Stiftungen …)
  - Kapitalgesellschaften (AG, GmbH, Kommandit- & Kollektivgesellschaften ….)

Grosser Unterschied:

- Öffentlich-rechtliche Körperschaften unterstehen der (kantonalen, kommunalen oder bundesrechtlichen) **Archivgesetzgebung**.
- Private Unternehmen nicht, sofern sie nicht öffentlich-rechtliche Aufgaben erfüllen (z.B. Leistungsauftrag des Kantons)

Für jede Organisationsform und jede Branche sind nebst den **allgemeinen gesetzlichen Grundsätzen** jedoch immer die spezifischen

- branchenspezifischen **Gesetzesgrundlagen**
- **Standards & Normen**
- **Risikosituationen**

zu berücksichtigen und anzuwenden.

Governance

- Governance
  - Ausgangslage
  - Vom Stellenwert der Informationen
  - Von den Sorgfaltspflichten der Führungskräfte
  - Von den gesetzlichen Grundlagen
  - Von den gesetzlichen Aufbewahrungsfristen
  - Von den selbstregulatorischen Vorgaben
  - Spezialrechtliche Gesichtspunkte (elektronische Signaturen)
- Beweiswert nachträglich eingescannter Dokumente

Risikosituationen

Bedrohungen für Geschäftsinformationen

Cyberangriff auf Comparis

Comparis-Hacker hatten Zugang zu Nutzerdaten

Aktualisiert um 08:28 Uhr

https://www.srf.ch/news/wirtschaft/cyberangriff-auf-comparis-comparis-hacker-hatten-zugang-zu-nutzerdaten

Cyberkriminalität

Emil Frey-Gruppe wurde Opfer von Cyberangriff

Mittwoch, 12.01.2022, 01:44 Uhr

https://www.srf.ch/news/schweiz/cyberkriminalitaet-emil-frey-gruppe-wurde-opfer-von-cyberangriff

Hacker legen einzige Zeitungspapierfabrik der Schweiz lahm – Folgen nicht absehbar

https://www.watson.ch/digital/schweiz/744582672-hacker-legen-einzige-zeitungspapierfabrik-der-schweiz-lahm-mit-folgen

Hackerangriff auf die Rothenburger Auto AG Group

Die Auto AG Group mit Sitz in Rothenburg wurde Opfer eines Hackerangriffs. Die Täterschaft ist bisher unbekannt.

27.08.2019, 17.26 Uhr

Merken Drucken Teilen

Das Gebäude der Auto AG Group in Rothenburg. (Bild: Nadia Schärli, Rothenburg, 16. April 2019)

Bedrohungen für Geschäftsinformationen

https://www.srf.ch/news/schweiz/cyberkriminalitaet-hackerangriff-auf-die-gemeinde-montreux

News > Schweiz >

Cyberkriminalität

Hackerangriff auf die Gemeinde Montreux

Montag, 11.10.2021, 08:17 Uhr
Aktualisiert um 11:33 Uhr

Dieser Artikel wurde **4**-mal geteilt.

- Die Waadtländer Gemeinde Montreux ist Ziel eines Cyberangriffs geworden.
- Die Attacke sei am Sonntagmorgen entdeckt worden, teilte die Gemeinde mit. Die Grösse des Angriffs und der Schaden können erst jetzt eingeschätzt werden, teilt die Gemeinde mit.

Governance & Compliance

Corporate Governance

Corporate Governance (deutsch: Grundsätze der Unternehmensführung) bezeichnet den Ordnungsrahmen für die Leitung und Überwachung von Unternehmen.[1][2] Der Ordnungsrahmen wird maßgeblich durch Gesetzgeber und Eigentümer bestimmt. Die konkrete Ausgestaltung obliegt dem Aufsichts- bzw. Verwaltungsrat und der Unternehmensführung.

Das unternehmensspezifische Corporate Governance-System besteht aus der Gesamtheit relevanter Gesetze, Richtlinien, Kodizes, Absichtserklärungen, Unternehmensleitbild, und Gewohnheit der Unternehmensleitung und -überwachung.

Governance & Compliance (2)

Compliance bzw. **Regeltreue** (auch Regelkonformität) ist in der betriebswirtschaftlichen und rechtlichen Fachsprache der Begriff für die **Einhaltung von Gesetzen und Richtlinien**, aber auch von **freiwilligen Standards, Normen oder Codices**, in Unternehmen.

Die Gesamtheit der Grundsätze und Massnahmen eines Unternehmens zur Einhaltung bestimmter Regeln und damit zur Vermeidung von Regelverstössen in einem Unternehmen wird als „**Compliance Management System**“ bezeichnet.

Corporate Governance (CG)

CG ist das Konzept einer **gesamtheitlichen**, **verantwortungsbewussten** und **wertschöpfungsorientierten Unternehmensführung**, indem diese den unterschiedlichen Interessen der Öffentlichkeit, des Staates, der Aktionäre, der Mitarbeiter, der Zulieferer und anderer Stakeholder Rechnung trägt.

Im engeren Sinne bedeutet Corporate Governance die **rechtliche** und **institutionell einwandfreie Geschäftsführung** mit entsprechenden **Kontrollmechanismen**, die eine ausreichende Entschädigung der Risikokapitalgeber sicherstellen soll.

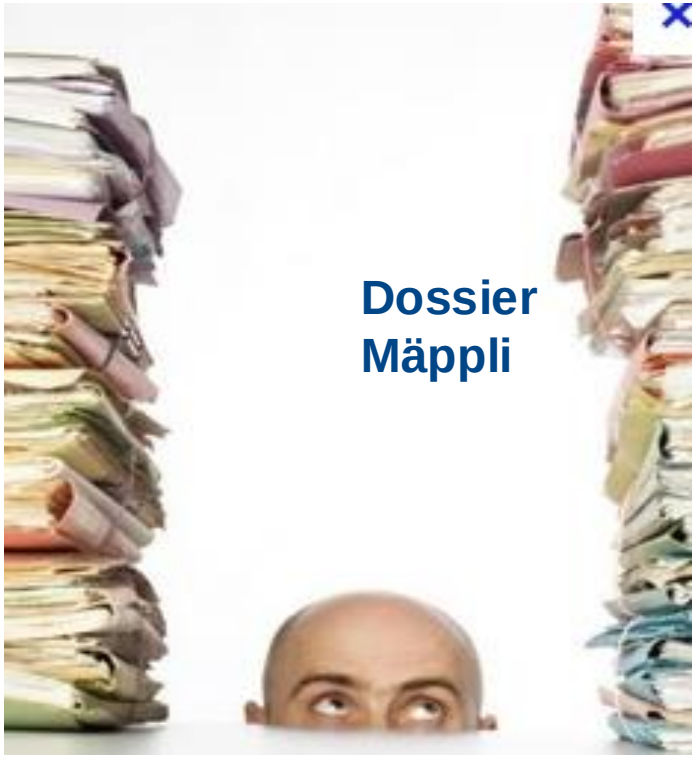
Teil 1 Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.1. Ausgangslage

Information-Management

Geschäftsverwaltung – Verwalten von Geschäften



Informations-Management

Vor 30 Jahren

„Sie haben irgendwann die Schreibmaschine durch den Computer ersetzt....

.... sonst ist alles beim Alten geblieben.“

Information-Management

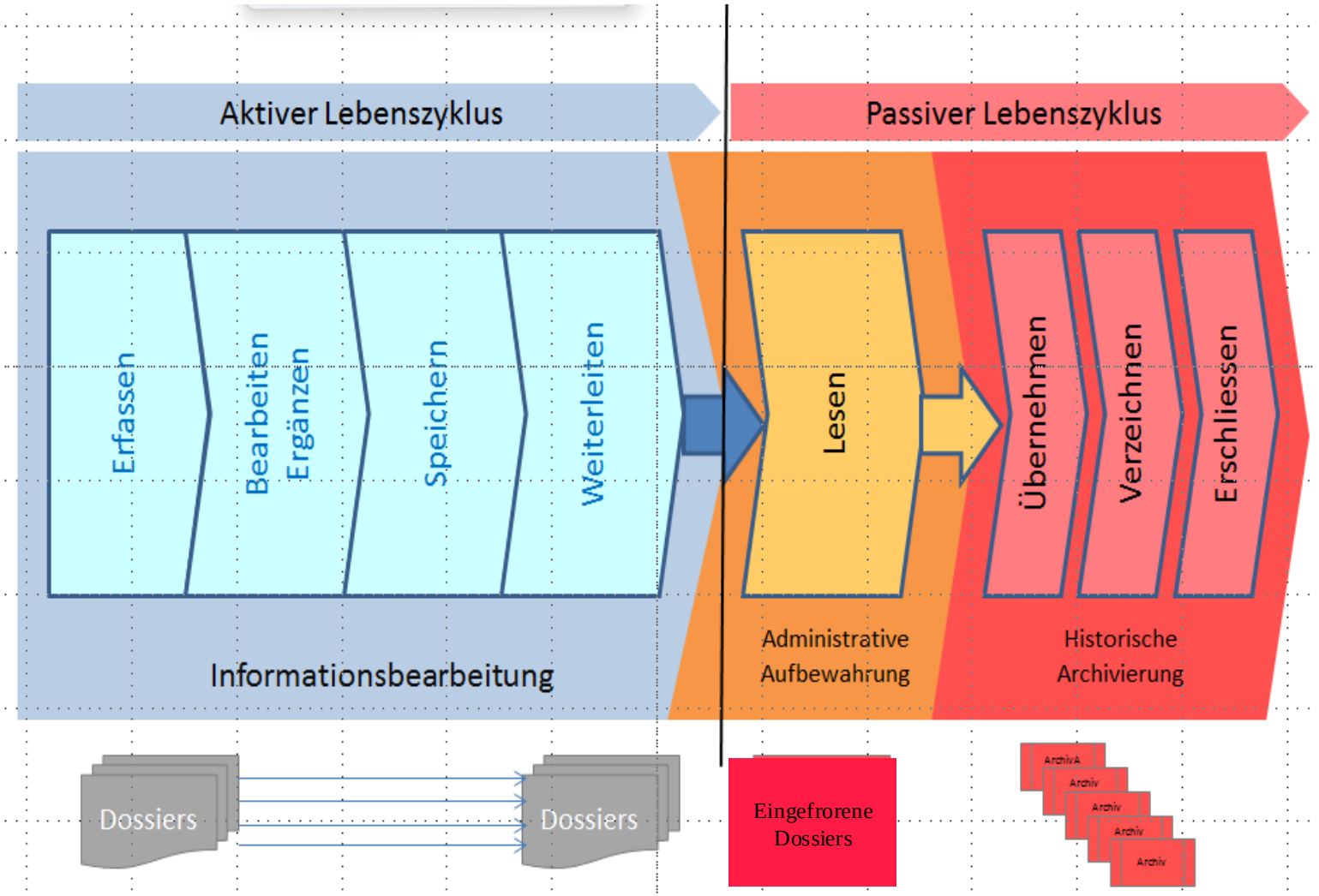
Strukturierte und unstrukturierte Daten

unstrukturiert

- Einwohnerkontrolle
- Objektwesen
- Finanzapplikationen
- KliB
- Steuern
- ……
- ……

strukturiert

Information-Management



Teil 1 Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.2. Vom Stellenwert der Informationen im Unternehmen und in der Verwaltung

Information

- Wissen - Daten - Argumente – Entscheide – Verfügungen – Urteile .....
- Unterlagen - Pläne - Konstruktionen - Forschungsergebnisse - Verträge - QS-Kennzahlen.....
- Informationen an Parlamente, Kommissionen, Aufsichtsgremien etc.
- Unterlagen - Kommunikation intern / extern.....

- **Alle Prozesse generieren Informationen** (Daten- oder Unterlagen-Records)

- In jeder Form..... (papierbezogen, digital)
- In jedem Format..... (Office - Audio - Video - SMS - eMail - Internet)

Informationen - Geschäftsrelevanz

- Heute: „informationsorientierte Organisationen“
- > 90% Schriftgut ist heute digitalisiert

- **Ohne (digitale) Informationen ist das Unternehmen tot**

- **Informationen** sind **strategische Grundbausteine** für die UN-Führung
- **Informationen** sind der **operative Kernbrennstoff** für Unternehmen/Verwaltungen und ihre Leistungserbringung/Aufgabenerfüllung

- Durchsetzung von Rechtsansprüchen hängt von zeitgerechter Bereitstellung **beweistauglicher und revisionssicherer Informationen** ab.

- Sicherstellung der Business Continuity (Arbeiten ohne Zugriff auf elektronische Akten) gehört zu den erweiterten Führungsaufgaben.

Entwicklungen

- **Allgemein**
  - Aufgabenerfüllung hängt von **zeitgerechter, vollständigen und unveränderten Bereitstellung und Verfügbarkeit von Informationen** ab.
- **Verwaltungen**
  - eGov-Strategie CH: medienbruchfreier Informationsaustausch über staatliche Hierarchiestufen wird zur Kernherausforderung der Zukunft / Einbindung von Bürgern, Unternehmen und anderen Verwaltungen (z.B. Kanton <-> Gemeinden).
  - Leistungs- & Eingriffsverwaltung muss ihre Entscheide **nachvollziehbar** begründen
  - Alle Entscheide der Verwaltung sind über Rechtsmittel anfechtbar
  - Öffentlichkeitsprinzip führt zur Öffnung der Informationsgefässe der Verwaltungen
  - eCH-Standards: (eCH-0002: Records Management; eCH-0160: Archivische Ablieferungsschnittstelle SIP in das digitale Langzeitarchiv)
- **Unternehmen**
  - Unternehmen unterliegen einer stetigen Zunahme von Regulierungen (Compliance)
  - Nichteinhaltung führt zu Bussen (Banken), Wettbewerbsnachteilen, Zulassungsbeschränkungen; Ausschluss in öffentlichen Ausschreibungen (Eignungskriterium ISO 15489; ISO 14721).

Geschäftsrelevante Informationen

Grundsätzlich können alle Informationen auf irgendwelchen Informationsträgern für ein Unternehmen oder die Verwaltung **geschäftsrelevant** sein oder **erst später** (!) **geschäftsrelevant werden**.

Papier, elektronische Daten, Audiodaten, Videodaten, eMail, SMS, WhatsApp etc.

Immer wenn **Rechte oder Pflichten begründet, geändert oder aufgehoben** werden, handelt es sich um **geschäftsrelevante Informationen**.

Immer wenn das Unternehmen (die GL oder der VR) oder der Staat **sorgfältiges** und/oder **gesetzeskonformes Handeln nachweisen oder beweisen** müssen, ist Handlungsbedarf angezeigt.

Information-Management

Das Management von Informationen – in welcher Form und auf welchen Medien auch immer – wird zum **kritischen Erfolgsfaktor** für die Unternehmung/Verwaltungstätigkeit der Zukunft.

Ohne Records Management, Ordnungssysteme und Dossierbildung ist auch das eGovernment der Zukunft in der Verwaltung undenkbar.

Unternehmen **verlieren** ihre **Rechtsdurchsetzungsfähigkeiten**, wenn zwischen vorgegebener, elektronischer Informationsverarbeitung und faktisch gelebter Papieraufbewahrung ein nicht ordnungsgemäss definierter Umgang mit dem gesamten geschäftsrelevanten Schriftgut zugelassen wird. Hybride Informationsbestände sind gefährlich.

Teil 1: Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.3. Grundlagen der Sorgfaltspflicht im Umgang mit Informationen

Corporate Governance (2)

- Vom Verwaltungs- oder Unternehmens-Management (VR & GL) gefordert sind bezüglich **geschäftsrelevanter Informationen**

  - **geordnete Führung**
  - **rechtskonforme Aufbewahrung** und
  - **zeitgerechte Verfügbarkeit**
  - **Nachweisbarkeit und Beweistauglichkeit**
  - **Allenfalls deren Revisionssicherheit**

Corporate Governance (3)

Geordnete Führung der geschäftsrelevanten Informationen

- **gesetzeskonform**
- **risikobezogen**
- wirtschaftlich vertretbar
- **revisionssicher**
- **beweistauglich**
- zeitgerecht

Unübertragbare Aufgaben

**Bundesgesetz
betreffend die Ergänzung
des Schweizerischen Zivilgesetzbuches
(Fünfter Teil: Obligationenrecht)**

vom 30. März 1911 (Stand am 1. August 2008)

Art. 716a OR

[1] Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[2] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

Zivilrechtliche Verantwortung VR & GL

CONFOEDERATIO HELVETICA

Die Bundesbehörden der Schweizerischen Eidgenossenschaft

- Organisationsverantwortung als unübertragbare und unentziehbare Aufgabe des Verwaltungsrates (Art. 716a Abs. 1 und 2 OR)
- Complianceverantwortung des VR (Art. 716a Abs. 1 OR)
- Unternehmensverantwortung des VR (Art. 716a Abs. 1 OR)
- Verantwortung für Personalauswahl des VR (Art. 716a Abs. 4 OR)
- Führungsverantwortung des VR (Art. 716a Abs. 5 OR)

Check & balances

Das geltende schweizerische Aktienrecht trägt mit drei zentralen Artikeln (OR Art. 716a, 716b und 717) diesen Forderungen nach „checks and balances“, klar festgehaltener **Eigenverantwortung des Verwaltungsrats**, interner **Berichterstattung** und Beachtung der **Treuepflicht** bereits in moderner Art Rechnung.

Art. 754 OR

Haftung des Verwaltungsrates und der Geschäftsleitung für Verwaltung, Geschäftsführung und Liquidation

Verantwortung von Dienststellenleitern (öV)

Der Amtsvorsteher ist für die Erfüllung aller Aufgaben des Amtes verantwortlich. Seine Hauptaufgabe:

- Er erarbeitet und kontrolliert die Einhaltung der konzeptionellen und strategischen Grundsätze des Informatik-Einsatzes.
- Er erstellt einen rollenden, mehrjährigen strategischen Informatik-Plan (SIP) und den jährlichen Informatik-Voranschlag.
- Er berät den Regierungsrat in allen Organisations- und Informatik-Fragen.
- Er vertritt die Organisations- und Informatik-Interesse in verwaltungsinternen und -externen Kommissionen und Arbeitsgruppen.
- Er arbeitet mit allen Ämtern der Staatsverwaltung sowie rechtliche selbstständigen Anstalten zusammen, soweit dies erforderlich ist.
- Er legt die Organisation des Amtes fest und umschreibt die Aufgaben, Befugnisse und verantwortung der einzelnen Abteilungen.
- Er genehmigt die Pflichtenhefte der Mitarbeiter des Amtes, erstellt mit den Abteilungsleitern die Aus- und Weiterbildungspläne und definiert die Führungsrichtlinien innerhalb des Amtes.
- Er trifft alle Entscheide im Zuständigkeitsbereich des Amtes, soweit diese nicht einer Abteilung oder dem Amtssekretariat übertragen wird.
- Im Rahmen der Amtsleitung verteilt er die Projekte inkl. Kompetenzen und Verantwortung auf die einzelnen Abteilungen.
- Er überwacht zusammen mit dem Benutzer die Wirtschaftlichkeit, Effizienz und Effektivität des Mitteleinsatzes in der Organisation und Informatik.
- Er definiert und realisiert ein aussagefähiges Informatik-Controlling-System.
- Er koordiniert sämtliche Verträge im Bereich der Amtsstelle mit dem Rechtsdienst des Finanz-Departementes.

Delegationsgrundsatz

Führungskräfte können

Aufgaben delegieren

- Innerhalb GL
  Mitarbeitende
- Externe Dritte
  (z.B. Datenverarbeiter)

Die Verantwortung aber NIE

→ Art. 754 OR

Teil 1: Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.4. Gesetzliche Grundlagen

AG: Befugnisse der Generalversammlung

Dritter Abschnitt: Organisation der Aktiengesellschaft

A. Die Generalversammlung

Art. 698

I. Befugnisse

[1] Oberstes Organ der Aktiengesellschaft ist die Generalversammlung der Aktionäre.

[2] Ihr stehen folgende unübertragbare Befugnisse zu:

1. die Festsetzung und Änderung der Statuten;
2. die Wahl der Mitglieder des Verwaltungsrates und der Revisionsstelle;
3. [392] die Genehmigung des Lageberichts und der Konzernrechnung;
4. die Genehmigung der Jahresrechnung sowie die Beschlussfassung über die Verwendung des Bilanzgewinnes, insbesondere die Festsetzung der Dividende und der Tantieme;
5. die Entlastung der Mitglieder des Verwaltungsrates;
6. die Beschlussfassung über die Gegenstände, die der Generalversammlung durch das Gesetz oder die Statuten vorbehalten sind.[393]

Aktionäre – Aktionariat
Oberstes Organ

Art. 716*a*[430]

2. Unübertragbare Aufgaben

[1] Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[431] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

[2] Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.

AG: VR Compliance-Verantwortung

B. Der Verwaltungsrat[414]

5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;

Compliance-Verantwortung

Gesetzliche Grundlage

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

Art. 754[475]

[1] Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

[2] Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Zivilrechtliche Verantwortung VR & GL (3)

Umkehr der Beweislast zulasten VR und GL-Mitglieder

Nachweis der „gehörigen“

- Auswahl (cura in eligendo) Kommandieren
- Unterrichtung (cura in instruendo) Kontrollieren
- Überwachung (cura in custodiendo) Korrigieren

Nachweisdokumente = rechtskonform und beweistauglich aufbewahrte Informationen

Gesetzeskonformes Information-Management ist die **Lebensversicherung für die Führungskräfte**

Obligationenrecht

Art. 957*a*

B. Buchführung

[1] Die Buchführung bildet die Grundlage der Rechnungslegung. Sie erfasst diejenigen Geschäftsvorfälle und Sachverhalte, die für die Darstellung der Vermögens-, Finanzierungs- und Ertragslage des Unternehmens (wirtschaftliche Lage) notwendig sind.

[2] Sie folgt den Grundsätzen ordnungsmässiger Buchführung. Namentlich sind zu beachten:

1. die vollständige, wahrheitsgetreue und systematische Erfassung der Geschäftsvorfälle und Sachverhalte;
2. der Belegnachweis für die einzelnen Buchungsvorgänge;
3. die Klarheit;
4. die Zweckmässigkeit mit Blick auf die Art und Grösse des Unternehmens;
5. die Nachprüfbarkeit.

Strafrecht

Dritter Teil: Begriffe

Art. 110

4 *Urkunden* sind Schriften, die bestimmt und geeignet sind, oder Zeichen, die bestimmt sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient.

Urkundenfälschung mit digitalen Daten

Schweizerisches Strafgesetzbuch **311.0**

vom 21. Dezember 1937 (Stand am 1. Januar 2013)

Elfter Titel: Urkundenfälschung

Art. 251[193]

1. Wer in der Absicht, jemanden am Vermögen oder an andern Rechten zu schädigen oder sich oder einem andern einen unrechtmässigen Vorteil zu verschaffen,

eine Urkunde fälscht oder verfälscht, die echte Unterschrift oder das echte Handzeichen eines andern zur Herstellung einer unechten Urkunde benützt oder eine rechtlich erhebliche Tatsache unrichtig beurkundet oder beurkunden lässt,

eine Urkunde dieser Art zur Täuschung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

Urkundenfälschung mit digitalen Daten

Schweizerisches Strafgesetzbuch **311.0**

vom 21. Dezember 1937 (Stand am 1. Januar 2013)

Art. 317[286]

1. Beamte oder Personen öffentlichen Glaubens, die vorsätzlich eine Urkunde fälschen oder verfälschen oder die echte Unterschrift oder das echte Handzeichen eines andern zur Herstellung einer unechten Urkunde benützen,

Beamte oder Personen öffentlichen Glaubens, die vorsätzlich eine rechtlich erhebliche Tatsache unrichtig beurkunden, namentlich eine falsche Unterschrift oder ein falsches Handzeichen oder eine unrichtige Abschrift beglaubigen,

werden mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

E-Mails sind Urkunden (1)

Bundesgericht Tribunal federal Tribunale federale Tribunal federal

Urtellskopf

138IV 209

31.Auszug aus dem Urteil der Strafrechtlichen Abteilung i.S.X. gegen Staatsanwaltschaft Basel Landschaft (Beschwerde in Strafsachen) vom 22. Oktober 2012

Regeste

Art. 110 Abs. 4 und Art. 251 Ziff. 1 StGB;

Urkundenqualität eines E-Mails.

E-Mails sind Computerurkunden.Verfälscht der Täter an ihn gerichtete E-Mails und leitet sie anschliessend an Drittpersonen weiter, erfüllt er den Tatbestand der Urkundenfälschung.

E-Mails sind Urkunden (2)

Bundesgericht
Tribunal federal
Tribunale federale
Tribunal federal

5.4 Der Schuldspruch wegen Urkundenfälschung verletzt kein Bundesrecht.

Ausser Frage steht zunächst,dass E-Mails Urkunden darstellen,wenn sie beim Empfänger ausgedruckt werden,d.h. wenn die Daten sichtbar gemacht werden,sofem der Aussteller erkennbar ist (vgl. **BGE 116 IV 343** E. 3).

Wie die Vorinstanz zutreffend annimmt,kommt aber auch dem noch nicht ausgedruckten E-Mailgrundsätzlich der Charakter einer (Computer-)Urkunde zu. Dabei erfüllt die Verfälschung eines E-Mails ohne weiiteres den Tatbestand der Urkundenfälschung,soweit dieses nach der Manipulation weiterversendet wird und seinen Adressaten erreicht. Der Täter setzt dadurch einen Prozess in Gang,der die Speicherung der Datenurkunde zur Folge hat.

BGE 138 IV 209 S.213

Organisationsmangel

Sozialversicherungsgericht des Kantons Zürich

II. Kammer

Urteil vom 10. Januar 2006 (IV.2005.01047)

in Sachen

S.___

Beschwerdeführer

2.3 Für jedes Sozialversicherungsverfahren sind alle Unterlagen, die massgeblich sein können, vom Versicherungsträger systematisch zu erfassen (Art. 46 ATSG). Dies setzt voraus, dass die Aktenführung nach festgelegten, allgemeinen, sachgerechten und zweckmässigen Kriterien erfolgt (Kieser, ATSG-Kommentar, N 10 zu Art. 46).

Im Weiteren bleibt zu bemerken, dass es der Beschwerdegegnerin offenbar möglich ist, ihre mit dem ELAR-System erfassten Akten beim Ausdruck zu nummerieren. Denn jedes der dem Gericht eingereichten Aktenstücke trägt in der Fusszeile eine Nummerierung sowie die Angabe zu den Seitenzahlen (vgl. Urk. 8/1-113). Es ist daher nicht einzusehen,

Organisationsmangel

weshalb diese Art der Aktenführung nicht auch im Rahmen der Akteneinsicht im Verwaltungsverfahren gewährleistet wird, zumal eine solche EDV-mässige Nummerierung auch im Massengeschäft kaum grösseren Aufwand für die Beschwerdegegnerin bedeutet.

Zusammenfassend ist somit festzuhalten, dass die Beschwerdegegnerin mit der Art der hier gewährten Akteneinsicht die Gehörsrechte des Beschwerdeführers verletzt hat. Dieser Mangel ist derart schwer, dass er nicht im vorliegenden Verfahren geheilt werden kann. Die Sache ist daher an die Beschwerdegegnerin zurückzuweisen, damit sie dem Beschwerdeführer im Verwaltungsverfahren gehörig Akteneinsicht gewährleiste und hernach neu entscheide.

Teil 1: Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.5. Gesetzliche Aufbewahrungsfristen

Grundprinzipien der Aufbewahrung

**Bundesgesetz
betreffend die Ergänzung
des Schweizerischen Zivilgesetzbuches
(Fünfter Teil: Obligationenrecht)**

Art. 958*f*

E. Führung und Aufbewahrung der Geschäftsbücher

1 Die Geschäftsbücher und die Buchungsbelege sowie der Geschäftsbericht und der Revisionsbericht sind während zehn Jahren aufzubewahren. Die Aufbewahrungsfrist beginnt mit dem Ablauf des Geschäftsjahres.

Vorbehalten bleiben branchenspezifische, gesetzliche Aufbewahrungsfristen

- z.B. Ingenieure im Brückenbau (25 Jahre Plan- und Berechnungsunterlagen)
- Pharmabranche (Forschungsergebnisse, Langzeitstudien)

Aufbewahrungsfristen

Merkpunkte zu gesetzlichen Aufbewahrungsfristen

- sind immer **nur Minimalaufbewahrungsfristen**

- allenfalls längerer Aufbewahrungsbedarf in Verwaltung oder Unternehmen (ergibt sich aus eigener Risikoanalyse)

- keine automatisierten File-Löschungsmechanismen auf Fristende vorsehen (Prozessrisiko)

Spielbankenrecht

Art. 30 Dokumentationspflicht

[1] Die Spielbank hat **Protokolle zu führen**, die Rückschlüsse auf den internen Geldfluss sowie auf Handlungen an Spieltischen, Glücksspielautomaten und Jackpot-Systemen und Eingriffe in diese zulassen.

Art. 34 Aufbewahrungsdauer

Die Protokolle nach den Artikeln 30 und 31 sind **fünf Jahre an einem sicheren Ort aufzubewahren**, soweit andere Bundesgesetze keine längeren Fristen vorsehen. Die Kommission kann für einzelne Protokolle die Frist verkürzen oder bis auf zehn Jahre verlängern.

Geldwäscherei-Gesetz

Art. 7 Dokumentationspflicht

[1] Der Finanzintermediär muss über die getätigten Transaktionen und über die nach diesem Gesetz erforderlichen Abklärungen Belege so erstellen, dass fachkundige Dritte sich ein zuverlässiges Urteil über die Transaktionen und Geschäftsbeziehungen sowie über die Einhaltung der Bestimmungen dieses Gesetzes bilden können.

[2] Er **bewahrt die Belege so auf**, dass er allfälligen Auskunfts- und Beschlagnahmebegehren der Strafverfolgungsbehörden **innert angemessener Frist** nachkommen kann.

[3] Nach Beendigung der Geschäftsbeziehung oder nach Abschluss der Transaktion **bewahrt er die Belege mindestens während zehn Jahren auf**.

BVV2

831.441.1

**Verordnung
über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge
(BVV 2)**

vom 18. April 1984 (Stand am 1. Januar 2013)

Art. 27*j* Aufbewahrungsfrist

(Art. 41 Abs. 8 BVG)

1 Werden Vorsorgeleistungen ausgerichtet, dauert die Aufbewahrungspflicht für die Einrichtungen der beruflichen Vorsorge bis zehn Jahre nach Beendigung der Leistungspflicht.

2 Werden mangels Geltendmachung durch die versicherte Person keine Vorsorgeleistungen ausgerichtet, so dauert die Aufbewahrungspflicht bis zum Zeitpunkt, an dem die versicherte Person ihr 100. Altersjahr vollendet hat oder vollendet hätte.

Teil 1: Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.6. Selbstregulatorische Vorgaben

Geschäftsbücher-Verordnung

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

2. Abschnitt: Allgemeine Grundsätze

Art. 2 Grundsätze ordnungsgemässer Führung und Aufbewahrung der Bücher

[1] Bei der Führung der Geschäftsbücher und der Erfassung der Buchungsbelege sind die anerkannten kaufmännischen Grundsätze einzuhalten (ordnungsgemässe Buchführung).

[3] Die Ordnungsmässigkeit der Führung und der Aufbewahrung der Bücher richtet sich nach den anerkannten Standards zur Rechnungslegung, sofern die Gesetzgebung, insbesondere der 32. Titel des Obligationenrechts und diese Verordnung, nichts anderes vorsehen.[4]

Ordnungsmässigkeit

Art. 2 und 4 GeBüV (Geschäftsbücher-Verordnung SR 221.431)

Ordnungsmässigkeit (Art.2 GeBüV)

Gesetzgeber verweist ausdrücklich auch auf eine **„ordnungsgemässe Datenverarbeitung“**

- Branchenstandard,
- Empfehlungen der Bankenkommission,
- **internationale Standards**
  - **ISO 15489**, (eCH0002, eCH0039, eCH0160)
  - **ISO 14721** (Open archival informations system OAIS-Modell)
  - ISO 20652 (space data and information transfer systems producer-archive interface – Ablieferungsdefinition zwischen Produzent und Archiven)
  - **ISAD(G) International Standard Archival Description**, General Rules of the International Council on Archive (ICA)
  - **Schweiz:** Code of Conduct for corporate Governance von economiesuisse
  - eCH-Standard 0160 (Ablieferungsschnittstelle)

Nationaler Standard CH

economiesuisse

economiesuisse

economiesuisse

Deutsche Fassung

swiss code
of best practice
for corporate
governance

code suisse de bonnes
pratiques pour
le gouvernement
d'entreprise

English version

swiss code of best
practice for
corporate governance

Standards, Normen & Richtlinien

economiesuisse

Umgang mit Risiken und Compliance, internes Kontrollsystem

20

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes Risikomanagement und ein internes Kontrollsystem. Das Risikomanagement bezieht sich auf finanzielle, operationelle und reputationsmässige Risiken.

- Das interne Kontrollsystem ist der Grösse, der Komplexität und dem Risikoprofil der Gesellschaft anzupassen.
- Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab.
- Die Gesellschaft richtet eine interne Revision ein. Diese erstattet dem Prüfungsausschuss («Audit Committee») und gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.

Swiss Code of best practice for corporate governance

economiesuisse

	21
Der Verwaltungsrat trifft Massnahmen zur Einhaltung der anwendbaren Normen (Compliance).	– Der Verwaltungsrat ordnet die Funktion der Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien. – Er orientiert sich dabei an anerkannten Best Practice-Regeln.[3] – Der Verwaltungsrat gibt sich mindestens einmal jährlich darüber Rechenschaft, ob die für ihn und das Unternehmen anwendbaren Compliance-Grundsätze hinreichend bekannt sind und ihnen dauernd nachgelebt wird.

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

---

2. Abschnitt: Allgemeine Grundsätze

Art. 2 Grundsätze ordnungsgemässer Führung und Aufbewahrung der Bücher

[1] Bei der Führung der Geschäftsbücher und der Erfassung der Buchungsbelege sind die anerkannten kaufmännischen Grundsätze einzuhalten (ordnungsgemässe Buchführung).

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

---

[2] Werden die Geschäftsbücher elektronisch oder auf vergleichbare Weise geführt und aufbewahrt und die Buchungsbelege elektronisch oder auf vergleichbare Weise erfasst und aufbewahrt, so sind die Grundsätze der ordnungsgemässen Datenverarbeitung einzuhalten.[3]

[3] Die Ordnungsmässigkeit der Führung und der Aufbewahrung der Bücher richtet sich nach den anerkannten Standards zur Rechnungslegung, sofern die Gesetzgebung, insbesondere der 32. Titel des Obligationenrechts und diese Verordnung, nichts anderes vorsehen.[4]

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

Art. 8 Archiv

Die Informationen sind systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen. Zugriffe und Zutritte sind aufzuzeichnen. Diese Aufzeichnungen unterliegen derselben Aufbewahrungspflicht wie die Datenträger.

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

Art. 9 Zulässige Informationsträger

1 Zur Aufbewahrung von Unterlagen sind zulässig:

a. unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger;

b. veränderbare Informationsträger, wenn:

1. technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren),

2. der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z. B. durch «Zeitstempel»),

3. die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden, und

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

---

4. die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log files) ebenfalls aufbewahrt werden.

[2] Informationsträger gelten als veränderbar, wenn die auf ihnen gespeicherten Informationen geändert oder gelöscht werden können, ohne dass die Änderung oder Löschung auf dem Datenträger nachweisbar ist (wie Magnetbänder, magnetische oder magnetooptische Disketten, Fest- oder Wechselplatten, solid state-Speicher).

Geschäftsbücher-Verordnung (GebüV)

221.431

Verordnung
über die Führung und Aufbewahrung der Geschäftsbücher
(Geschäftsbücherverordnung; GeBüV)

vom 24. April 2002 (Stand am 1. Januar 2013)

Art. 10 Überprüfung und Datenmigration

1 Die Informationsträger sind regelmässig auf ihre Integrität und Lesbarkeit zu prüfen.

2 Die Daten können in andere Formate oder auf andere Informationsträger übertragen werden (Datenmigration), wenn sichergestellt wird, dass:

a. die Vollständigkeit und die Richtigkeit der Informationen gewährleistet bleiben; und

b. die Verfügbarkeit und die Lesbarkeit den gesetzlichen Anforderungen weiterhin genügen.

3 Die Übertragung von Daten von einem Informationsträger auf einen anderen ist zu protokollieren. Das Protokoll ist zusammen mit den Informationen aufzubewahren.

Teil 1: Governance & Compliance

im Umgang mit geschäftsrelevanten Informationen

1.7. Elektronische Signaturen

Einsatz von elektronischen Signaturen

Gesetzliche Grundlagen CH

Gesetze und Verordnungen

ZertES Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.03)

VZertES Verordnung vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032)

Verordnung des BAKOM vom 23. November 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (SR 943.032.1)

THG Bundesgesetz vom 6. Oktober 1995 über die technischen Handelshemmnisse (SR 946.51)

AkkBV Verordnung vom 17. Juni 1996 über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (SR 946.512)

Die elektronische Identität

für private Personen

Begriffe

Digitale Signatur

- „**Digitale Signatur**“ ist ein technischer Begriff. Damit ist ein mathematisches Verschlüsselungsverfahren gemeint.

Das Verfahren der digitalen Signatur kann beim Erstellen einer elektronischen Signatur zum Einsatz kommen – muss es aber nicht. Es gibt auch einfache Varianten elektronischer Signaturen, die ohne digitale Signatur auskommen.

Elektronische Signatur

- „**Elektronische Signatur**“ ist vor allem ein **juristischer Begriff**. Es geht hier um das **rechtsgültige und verbindliche Unterschreiben von Dokumenten auf elektronischem Weg**.

Das Gesetz unterscheidet hier zwischen verschiedenen Formen, die – je nach Dokument – die handschriftliche Unterschrift ersetzen bzw. nicht ersetzen können.

E-ID elektronischer Identitätsnachweis

Ein staatlich anerkannter elektronischer Identifikationsnachweis (E-ID) ermöglicht den Einwohnerinnen und Einwohnern der Schweiz online mittels eines digitalen Beweises die Identität zu belegen.

Gewährleistung

Die digitale Signatur stellt ein mathematisch-kryptografisches Verfahren dar, mit dem für eine bestimmte Nachricht Folgendes gewährleistet werden soll:

- **Authentizität**: Die Nachricht stammt nachweislich und unzweifelhaft von einem klar bestimmten Absender.

- **Integrität**: Die Nachricht wurde weder auf dem Transport noch nachträglich in irgendeiner Weise verändert.

PKI und CA

Die technische Infrastruktur, mit der die Schlüsselpaare erzeugt und bereitgestellt werden, heißt **Public Key Infrastructur (PKI).**

Ein wesentlicher Bestandteil der Public Key Infrastructur sind die **Zertifizierungsstellen (engl. Certification Authority, CA),** welche die Identität einer Person oder Organisation prüfen und dieser genau einen öffentlichen Schlüssel zuordnen.

Elektronische Signaturen – 3 Standards

Das Verfahren der digitalen Signatur wird unter anderem eingesetzt, um sichere, nachprüfbare Unterschriften auf dem elektronischen Weg zu erstellen.

Grundsätzlich ist es wichtig zu wissen, dass der **Gesetzgeber beim elektronischen Unterschreiben drei Standards** definiert:

Elektronische Signatur – EES

Einfache elektronische Signatur (EES): Dies kann bereits eine eingescannte Unterschrift oder eine angehängte E-Mail-Signatur sein.

Eine kryptografische Verschlüsselung (etwa durch eine digitale Signatur) ist nicht unbedingt notwendig.

EES enthält keine Elemente, welche die Authentizität und die Integrität eines elektronischen Dokumentes sicherstellen.

Elektronische Signatur - FES

Fortgeschrittene elektronische Signatur (FES): Hier kommt das Verfahren der digitalen Signatur zum Einsatz, da die Integrität des unterzeichneten Dokuments nachgewiesen werden und der Unterzeichnende eindeutig mit der Unterschrift verknüpft werden muss.

FES ist NIE der eigenhändigen Unterschrift gleichgestellt und kann daher dem digitalen Dokument keinen rechtsverbindlichen Charakter wie eine handschriftlich unterzeichnete Urkunde verleihen.

Elektronische Signatur - QES

Qualifizierte elektronische Signatur (QES) Auch hier wird das Verfahren der digitalen Signatur genutzt, um die Integrität des Dokuments und die Authentizität der Unterschrift zu gewährleisten.

Zusätzlich gelten weitere Sicherheitsanforderungen, etwa eine strengere Überprüfung der Identität des Unterzeichnenden (hochwertiges Onboarding-Verfahren) bei einer authorisierten Zertifizierungsstelle und der Einsatz eines Zeitstempels.

QES ist die **einzige elektronische Signatur**, welche vom Gesetzgeber der **eigenhändigen Unterschrift gleichgesetzt** wird (Art. 14bis Abs. 2 OR). Nur mit der QES können digitale Dokumente rechtskonform unterzeichnet werden.

Gesetzesgrundlage

Bundesgesetz
betreffend die Ergänzung
des Schweizerischen Zivilgesetzbuches
(Fünfter Teil: Obligationenrecht)

vom 30. März 1911 (Stand am 9. Februar 2023)

Zusatzanforderung Zeitstempel

QES

2bis Der eigenhändigen Unterschrift gleichgestellt ist die mit einem qualifizierten Zeitstempel verbundene qualifizierte elektronische Signatur gemäss Bundesgesetz vom 18. März 2016[4] über die elektronische Signatur. Abweichende gesetzliche oder vertragliche Regelungen bleiben vorbehalten.[5]

Nur für Privatpersonen

Elektronisch rechtsgültig unterzeichnet

Schweizerische Städte- und Gemeindeinformatik

SSGi

Lenkungsausschuss DecisionAdvisor
Verein SSGI / DV Bern AG / Mitglieder

An alle Teilnehmer gemäss separatem Verteiler

Verein SSGI
Präsident Lukas Fässler
Zugerstrasse 76B
6340 Baar

Telefon ++41 +41 727 60 80
Telefax ++41 +41 727 60 85

www.ssgi.ch
info@ssgi.ch
lfaessler@fsdz.ch

Zug, 27. Februar 2023

Sitzung Lenkungsausschuss DecisionAdvisor vom 9. März 2023, 14:00 – 16:30 Uhr,
Online Meeting unter Teilnahmelink: Hier klicken, um an der Besprechung teilzunehmen

Traktandenliste

1	Begrüssung und Zielsetzung / Vorstellung	Sitzungsleitung	**14:00**
2	Protokoll LAS Nr. 5 vom 27.09.2022	Sitzungsleitung	14:05 – 14:10
3	Rückblick und offene Punkte aus LAS September 2022	DV Bern AG	14:10 – 14:30
4	Bericht aus der ERFA-Gruppe	DV Bern AG	14:30– 14:50
	(Pause)		*14:50 – 15:00*
5	Allgemeine Entwicklung der Applikation DA	DV Bern AG	15:00– 15:25
6	Stand aktuelle Roadmap DA	DV Bern AG	15:25 – 15:40
7	Releaseplanung 2023	DV Bern AG	15:40 – 16:05
7	Varia	Alle	16:05 – 16:15
8	Termin LAS Nr. 7 September 2023	Alle	16:15 – 16:20
	Ende (inkl. Zeitreserve)		**16:30**

Allfällige Unterlagen befinden sich auf der SSGi-Plattform www.securesafe.ch unter «*Lenkungsausschuss DecisionAdvisor*». Im Übrigen werden alle Unterlagen als Präsentationen anlässlich der Sitzung von DV Bern präsentiert und anschliessend auf der SSGi-Plattform für alle Teilnehmer bereitgestellt. Sollten einzelne Teilnehmer noch keinen Zugang zur Plattform www.securesafe.ch haben, werden wir im Nachgang zur jeweiligen LAS neue Teilnehmer begleiten, damit sie eine direkte Anmeldung auf die Plattform von securesafe einrichten können. Auf jeden Fall notwendig für eine Teilnahme im Teamraum bei Securesafe.ch unter «*Lenkungsausschuss DecisionAdvisor*» ist eine kostenlose Erstanmeldung auf der Plattform von www.securesafe.ch, welche jeder Neuteilnehmer vorher selber sicherstellen muss (diese ist kostenlos).

Verein SSGI
Der Präsident

Rechtsanwalt
CH-6340 Baar (Schweiz), 28.02.2023

Lukas Fässler

QES Qualifizierte elektronische Signatur · Schweizer Recht
Signiert auf Skribble.com

Die elektronische Identität

für Unternehmen und Behörden

Elektronisches Siegel (2)

Bundesgesetz
über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate
(Bundesgesetz über die elektronische Signatur, ZertES)

vom 18. März 2016

Art. 2 Begriffe

In diesem Gesetz bedeuten:

d. *geregeltes elektronisches Siegel:* eine fortgeschrittene elektronische Signatur, die unter Verwendung einer sicheren Siegelerstellungseinheit nach Artikel 6 erstellt wurde und auf einem geregelten, auf eine UID-Einheit nach Artikel 3 Absatz 1 Buchstabe c des Bundesgesetzes vom 18. Juni 2010[3] über die Unternehmens-Identifikationsnummer (UIDG) ausgestellten und zum Zeitpunkt der Erzeugung des elektronischen Siegels gültigen Zertifikat beruht;

Weitere elektronische Signaturen (1)

Was in der analogen Welt der Firmenstempel oder Behördensiegel von Organisationen ist, wird jetzt mit Hilfe von dem

elektronischen Siegel

in das digitale Zeitalter übertragen.

Siegelnde Unternehmen können mit elektronischen Siegeln den **Herkunftsnachweis, Zeitpunkt, die Integrität und Authentizität** des Inhaltes einer digitalen Datei sicherstellen. Dabei basieren elektronische Siegel technisch auf dem gleichen Verfahren wie eine elektronische Signatur.

Elektronische Behördeneingaben

Verbindlicher digitaler Geschäftsverkehr

Elektronische Behördeneingaben

272.1

Verordnung
über die elektronische Übermittlung
im Rahmen von Zivil- und Strafprozessen sowie
von Schuldbetreibungs- und Konkursverfahren

vom 18. Juni 2010 (Stand am 1. Januar 2011)

Art. 4 Eingaben

Eingaben an eine Behörde sind an die Adresse auf der von ihr verwendeten anerkannten Zustellplattform zu senden.

Art. 6 Format

[1] Die Verfahrensbeteiligten haben ihre Eingaben einschliesslich Beilagen im Format PDF zu übermitteln.

Art. 7 Signatur

Als anerkannte elektronische Signatur im Sinne von Artikel 130 Absatz 2 ZPO, Artikel 33*a* Absatz 2 SchKG und Artikel 110 Absatz 2 StPO gilt eine qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin beruht.

Elektronische Behördeneingaben (2)

E-Justice

Im Rahmen verschiedener Gesetzgebungsprojekte des Bundes zu Gerichtsorganisation und Verfahren haben die Parteien seit Anfang 2011 die Möglichkeit, Eingaben bei Gerichten oder Behörden auch in elektronischer Form einzureichen. In zwei Verordnungen hat der Bundesrat geregelt, wie die Parteieingaben sowie der Versand der Urteile resp. Verfügungen in den verschiedenen Verfahren abgewickelt werden können. Um einer Behörde eine Eingabe zustellen zu können, müssen deren Adresse und allfällige Einschränkungen bekannt sein. Die Bundeskanzlei veröffentlicht deshalb im Internet Verzeichnisse der Behördenadressen:

Zivil- und Strafverfahren

Elektronische Eingabe - die kantonalen Behördenadressen.

Verwaltungsverfahren

Das Bundesverwaltungsgericht oder Behörden der dezentralen Bundesverwaltung können den elektronischen Verkehr für alle oder nur für bestimmte Verwaltungsverfahren zulassen auf.

Schuldbetreibung- und Konkursverfahren

Für die elektronische Übermittlung im Rahmen von Schuldbetreibungs- und Konkursverfahren sind die Behördenbriefkästen auf Online-Betreibungsschalter zu verwenden.

Zustellplattformen

Im Unterschied zum ungeschützten E-Mail-Verkehr wahrt die Zustellung über eine anerkannte Zustellplattform die Vertraulichkeit und Integrität der Dokumente.

Aktuell:
Projekt Justitia 4.0

Projekt zur Digitalisierung der Schweizer Justiz, indem Papierakten durch elektronische Akten ersetzt und der gesamte Rechts- und Aktenverkehr über die Plattform justitia.swiss abgewickelt werden soll

Elektronische Behördeneingaben (3)

ch.ch

Finden

DIE SCHWEIZER BEHÖRDEN ONLINE

Elektronische Eingabe bei Zivil- und Strafverfahren

Behördenadressen finden

Eidgenössische Gerichte

Bundesgericht
Bundesstrafgericht
Bundesverwaltungsgericht
Bundespatentgericht

Kantonale Gerichte

AG
AI
AR
BE
BL
BS
FR
GE
GL
GR
LU
JU
NE

ch.ch informiert auch über:

E-Justice

Bundesamt für Justiz - Elektronische Übermittlung

Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens

Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren

Elektronische Behördeneingaben (4)

Adressverzeichnis für den elektronischen Rechtsverkehr mit Behörden des Kantons LUZERN

Hintergrund: Elektronischer Rechtsverkehr .

Suche eGov Behörden (Beta):

Suche Behörden

(Verwende "?" für ein beliebiges Zeichen; "*" für eine unbestimmte Anzahl beliebiger Zeichen!)

Zurücksetzen | Alle Behörden

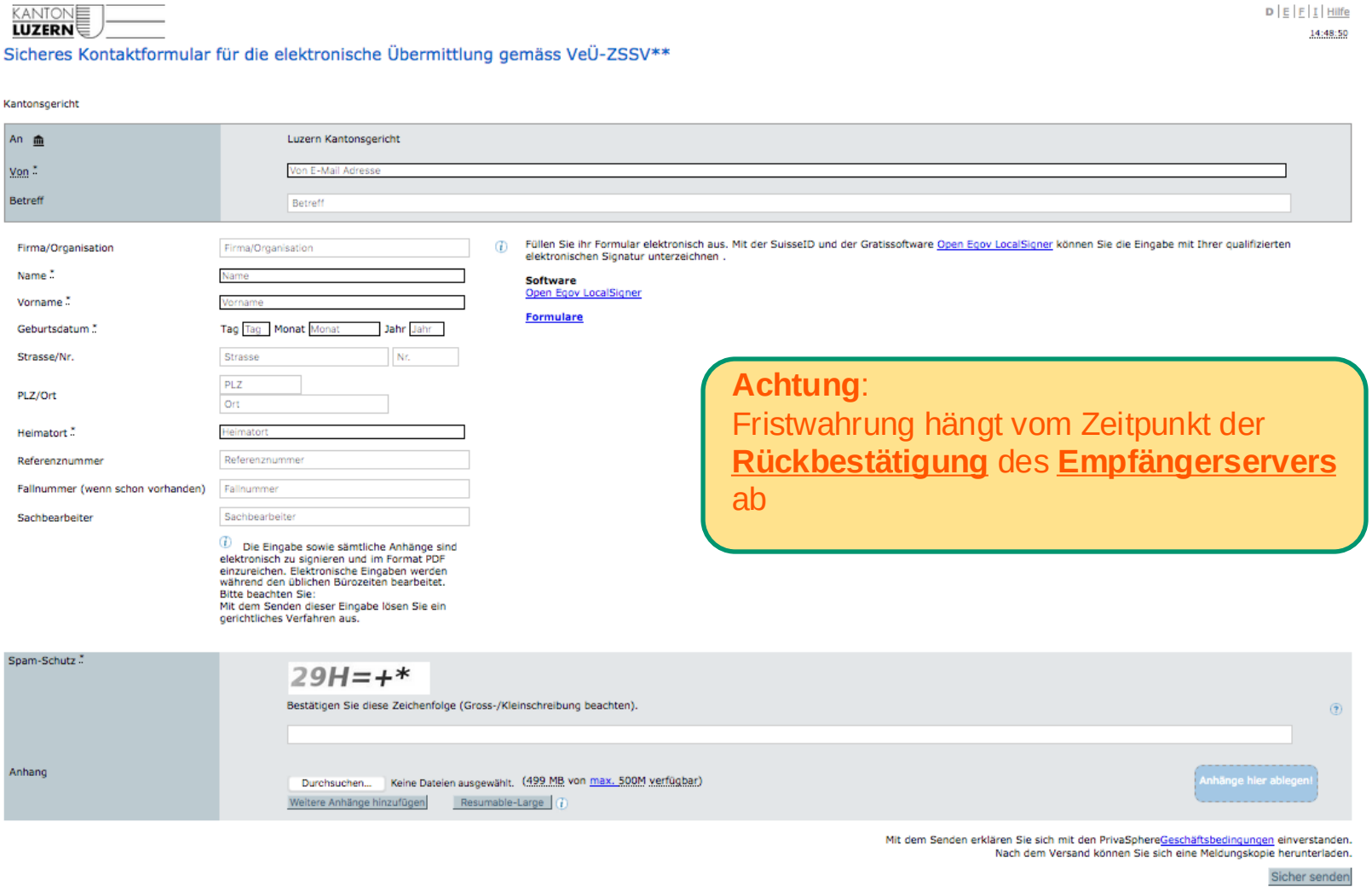
Hinweis - Suchbegriff "sg.ch" für St.Gallen, "ti.ch" für Ticino, "sem.admin.ch", etc.
Or "miet tg" to find all authorities related to "Miete" and "Thurgau".
In collaboration with https://www.ch.ch/de/e-justice/

.

Die Resultate für Ihren Suchbegriff "lu.ch" (31)

Name	Adresse
Kanton Luzern, Staatsanwaltschaft SA5 Staatsanwaltschaft Wirtschaftsde...	https://ees.lu.ch/staatsanwaltschaft-wirtschaftsdelikte
Luzern Kantonsgericht	https://eeg.lu.ch/kantonsgericht
Luzern Staatsanwaltschaft Zentrale Dienste	https://ees.lu.ch/staatsanwaltschaft-zentrale-dienste
Luzern Staatsanwaltschaft Spezialdelikte	https://ees.lu.ch/staatsanwaltschaft-spezialdelikte
Luzern Staatsanwaltschaft Sursee	https://ees.lu.ch/staatsanwaltschaft-sursee
Luzern Staatsanwaltschaft Emmen	https://ees.lu.ch/staatsanwaltschaft-emmen
Luzern Staatsanwaltschaft Kriens	https://ees.lu.ch/staatsanwaltschaft-kriens
Luzern Jugendanwaltschaft	https://ees.lu.ch/jugendanwaltschaft
Luzern Oberstaatsanwaltschaft	https://ees.lu.ch/oberstaatsanwaltschaft
Luzern Grundbuchamt Luzern West	https://eeg.lu.ch/grundbuchamt-west
Luzern Grundbuchamt Luzern Ost	https://eeg.lu.ch/grundbuchamt-ost
Luzern Konkursamt Willisau	https://eeg.lu.ch/konkursamt-west
Luzern Konkursamt Hochdorf	https://eeg.lu.ch/konkursamt-hochdorf
Luzern Konkursamt Kriens	https://eeg.lu.ch/konkursamt-kriens
Luzern Konkursamt Luzern	https://eeg.lu.ch/konkursamt-luzern
Luzern Friedensrichter Willisau	https://eeg.lu.ch/friedensrichter-willisau
Luzern Friedensrichter Hochdorf	https://eeg.lu.ch/friedensrichter-hochdorf

Elektronische Behördeneingaben (5)


KANTON LUZERN

D | E | F | I | Hilfe

14:48:50

Sicheres Kontaktformular für die elektronische Übermittlung gemäss VeÜ-ZSSV**

Kantonsgericht

An: Luzern Kantonsgericht

Von *: Von E-Mail Adresse

Betreff: Betreff

Firma/Organisation: Firma/Organisation

Name *: Name

Vorname *: Vorname

Geburtsdatum *: Tag Tag Monat Monat Jahr Jahr

Strasse/Nr.: Strasse Nr.

PLZ/Ort: PLZ Ort

Heimatort *: Heimatort

Referenznummer: Referenznummer

Fallnummer (wenn schon vorhanden): Fallnummer

Sachbearbeiter: Sachbearbeiter

Die Eingabe sowie sämtliche Anhänge sind elektronisch zu signieren und im Format PDF einzureichen. Elektronische Eingaben werden während den üblichen Bürozeiten bearbeitet.
Bitte beachten Sie:
Mit dem Senden dieser Eingabe lösen Sie ein gerichtliches Verfahren aus.

Füllen Sie ihr Formular elektronisch aus. Mit der SuisseID und der Gratissoftware Open Egov LocalSigner können Sie die Eingabe mit Ihrer qualifizierten elektronischen Signatur unterzeichnen .

Software
Open Egov LocalSigner

Formulare

Spam-Schutz *: 29H=+*

Bestätigen Sie diese Zeichenfolge (Gross-/Kleinschreibung beachten).

Anhang: Durchsuchen... Keine Dateien ausgewählt. (499 MB von max. 500M verfügbar)

Weitere Anhänge hinzufügen | Resumable-Large

Anhänge hier ablegen!

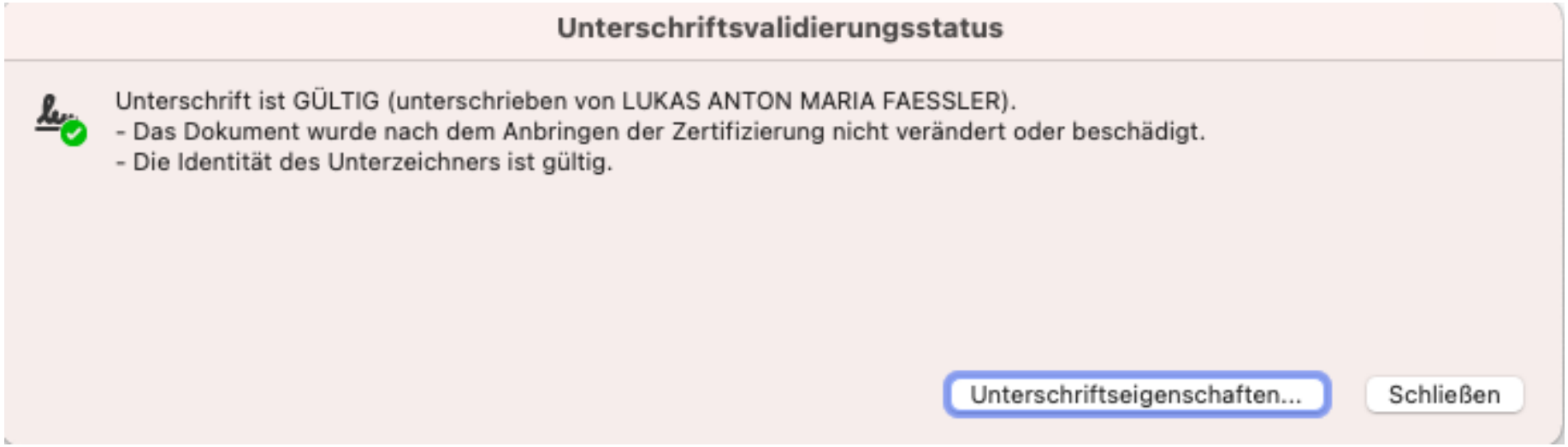
Mit dem Senden erklären Sie sich mit den PrivaSphereGeschäftsbedingungen einverstanden.
Nach dem Versand können Sie sich eine Meldungskopie herunterladen.

Sicher senden

Achtung:
Fristwahrung hängt vom Zeitpunkt der **Rückbestätigung** des **Empfängerservers** ab

Die Validierung von elektronischen Signaturen

Unterschrifts-Validierung in Signatur



Erste Validierung:
Durch direktes Anklicken der Signatur

Validatoren für elektronische Signaturen

https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation

EU-Validator

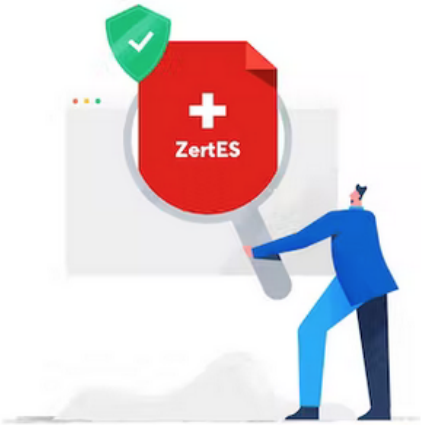
Für Signaturen nach EU-Recht (eIDAS)

Wir empfehlen den offiziellen QES-Validator der EU-Kommission (nur auf Englisch verfügbar).

Mit dem EU-Validator prüfen Sie, ob ein Dokument erfolgreich mit einer QES nach EU-Recht (eIDAS) signiert wurde.

CH-Validator

Für Signaturen nach Schweizer Recht (ZertES)

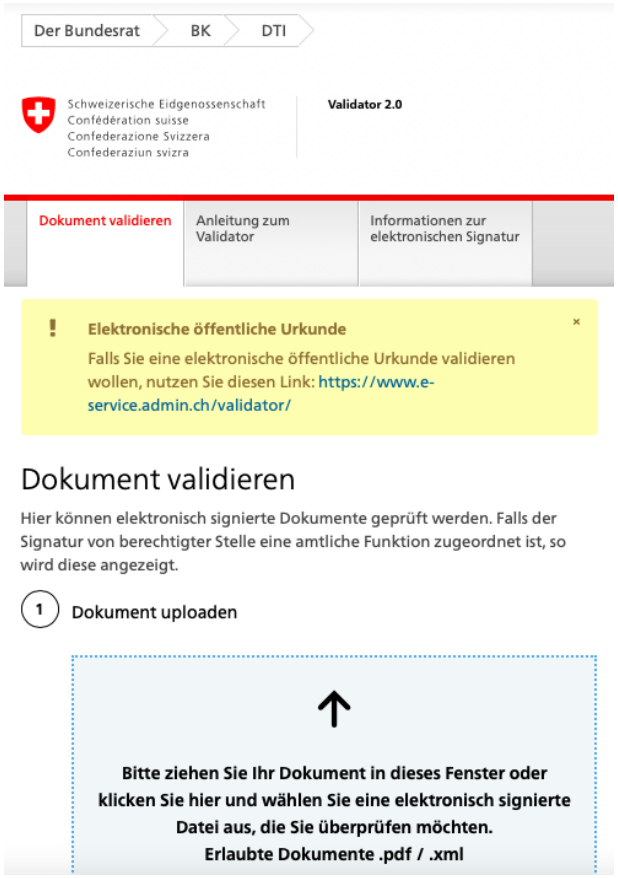


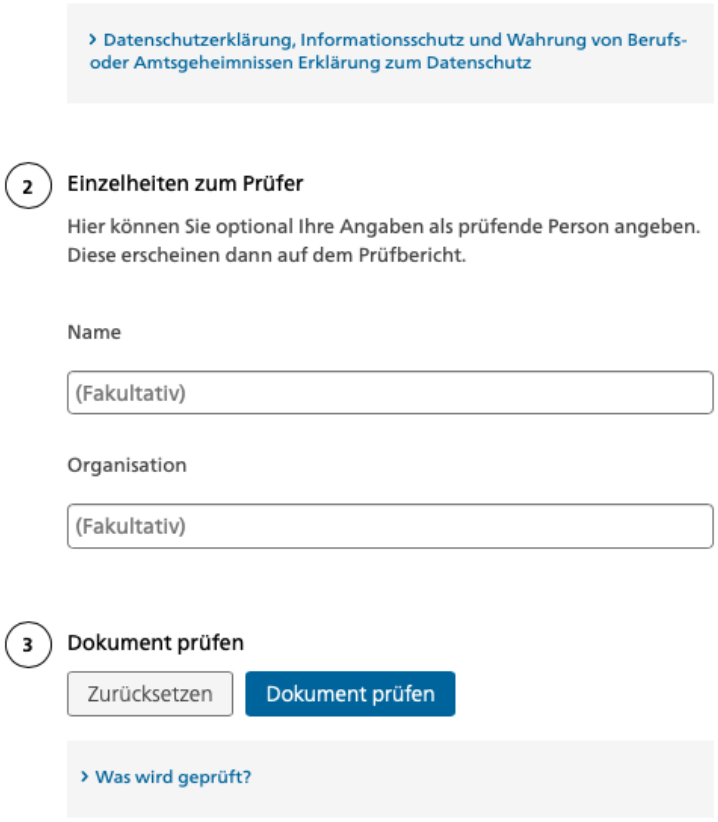
Wir empfehlen den offiziellen QES-Validator der Schweizer Bundesverwaltung.

Mit dem CH-Validator prüfen Sie, ob ein Dokument erfolgreich mit einer QES nach Schweizer Recht (ZertES) signiert wurde.

https://www.validator.admin.ch/

Der externe Validator des Bundes





Validator des Bundes

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Validator 2.0

Dokument validieren | Anleitung zum Validator | Informationen zur elektronischen Signatur

Kurzbericht

Prüfbericht für der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signatur gemäss ZertES und OR Art. 14 Abs. 2bis

Originaldokument anhängen

PDF Bericht herunterladen

Detailreport anzeigen

Neu beginnen

Dieser Prüfbericht gibt darüber Auskunft, ob jegliche elektronischen Signaturen auf dem geprüften Dokument der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signaturen sind. Das Vorhandensein eines qualifizierten Zeitstempels, der den genauen Signaturzeitpunkt nachweist, ist seit 01.01.2017 für jede der qualifizierten elektronischen Signaturen notwendig. Dokumente, die vor dem 01.01.2017 signiert wurden und keinen Zeitstempel tragen, sind in der Regel gültig, weil das ZertES damals keinen qualifizierten Zeitstempel verlangte. Aussagen zum Signaturzeitpunkt und Revokationsstatus sind damit aber nicht mit Sicherheit vertrauenswürdig.

Zusammenfassung der Dokumentprüfung

Das Dokument ist gültig signiert.

Das geprüfte Dokument trägt eine oder mehrere gültige der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signaturen gemäss ZertES und OR Art. 14 Abs. 2bis. Die Prüfergebnisse der einzelnen Signaturen sind im Detailbericht ersichtlich.

Folgende Prüfungen wurden durchgeführt:

- Das Dokument ist nach der letzten Signatur nicht mehr verändert worden.
- Alle validierten Signaturen des Dokumentes sind gültig gemäss ZertES.
- Alle zur Signatur verwendeten Zertifikate sind nicht revoziert, also gültig.
- Alle in diesem Dokument angebrachten Zeitstempel sind gültig gemäss ZertES.
- Alle in diesem Dokument für Signaturen verwendeten Zertifikate sind für diesen Dokumententyp legitimiert.

Anzahl Signaturen im Dokument: 1

Separater PDF-Bericht zum Download

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Prüfbericht für der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signatur gemäss ZertES und OR Art. 14 Abs. 2bis

Datum/Zeit der Prüfung:	01.03.2023 12:40:04 UTC
Name der signierten Datei:	Einladung und Traktandenliste - LAS Decision Advisor vom 09-03-2023 _signiert.pdf
Hash der Datei (SHA-256):	3f1193a3657a4551fe1d1c2baf6bfa52 bf0fc43c188f9c8cd522556386210453

Dieser Prüfbericht gibt darüber Auskunft, ob jegliche elektronischen Signaturen auf dem geprüften

Validierung elektronischer Signaturen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Prüfbericht für der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signatur gemäss ZertES und OR Art. 14 Abs. 2bis

Datum/Zeit der Prüfung:	11.01.2018 09:20:53 UTC
Angaben der prüfenden Person:	Rechtsanwalt Lukas Fässler, FSDZ Rechtsanwälte & Notariat AG
Name der signierten Datei:	Verjahrungsverzicht_V2 sign.pdf
Hash der Datei (SHA-256):	7cd60dddb7fb480f46aa2d452fe47e29 ff08d9f260bdd3907af35356d3843c20

Dieser Prüfbericht gibt darüber Auskunft, ob ein Dokument eine der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signatur trägt. Das Vorhandensein eines qualifizierten Zeitstempels, der den genauen Signaturzeitpunkt nachweist, ist seit 01.01.2017 notwendig.

Zusammenfassung der Dokumentprüfung

Das Dokument ist nicht gültig signiert.

Das geprüfte Dokument trägt keine der eigenhändigen Unterschrift gleichgestellte qualifizierte elektronische Signatur gemäss ZertES und OR Art. 14 Abs. 2bis.

Weitere elektronische Signaturen (2)

Elektronischer Zeitstempel

dienen dazu **elektronische Daten** einer

a. eindeutigen, **gesetzeskonformen Zeit** zuzuordnen
b. den **Nachweis** zu erbringen, dass diese **Daten nach dem Aufbringen des Zeitstempels nicht mehr verändert** wurden.

E-ID Bund

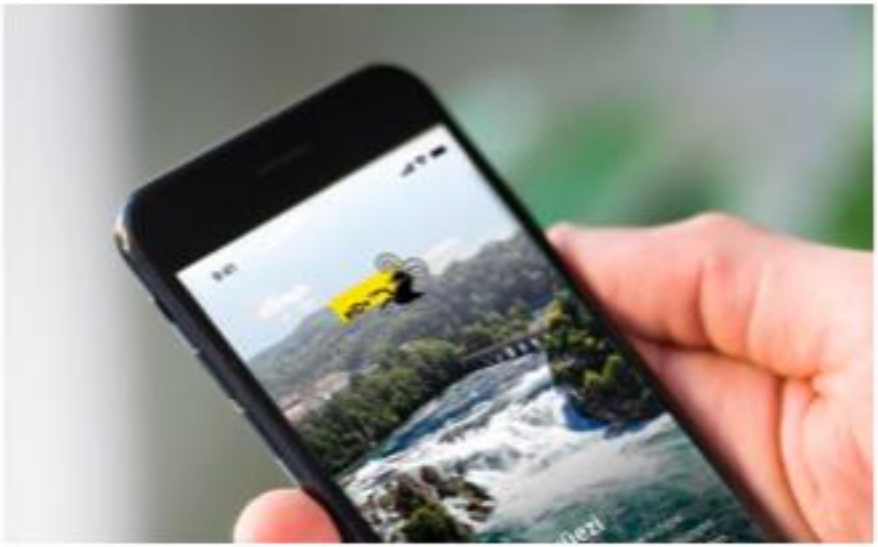
Ein staatlich anerkannter **elektronischer Identifikationsnachweis** (E-ID) ermöglicht den Einwohnerinnen und Einwohnern der Schweiz online mittels eines **digitalen Beweises die Identität zu belegen.**

Der Staat tritt dabei als Herausgeber der E-ID auf und sorgt für den Betrieb der nötigen Vertrauensinfrastruktur. Den Nutzerinnen und Nutzern soll grösstmögliche Kontrolle über ihre Daten ermöglicht werden.

Nur für natürliche Personen

https://www.youtube.com/watch?v=Lqv5kaU_-Hk

E-ID Gesetz am 8.3.2021 gescheitert (4)
Kantonale e-ID Schaffhausen seit 2017



Tätigen Sie online Behördengänge und sparen Sie so wertvolle Zeit. Dank der Schaffhauser eID+ können Kantonsbewohnerinnen und -bewohner auf ihrem Smartphone eine elektronische Identität einrichten und die darin erfassten Daten vom Einwohneramt offiziell staatlich bestätigen lassen. Die so erstellte Identität ermöglicht anschliessend einen sicheren und einfachen Zugriff auf verschiedene elektronische Behördendienstleistungen ohne zusätzliche Logins und Passwörter.

HIN-ID und Dokumente signieren (5)

HIN Sign

Dokumente fälschungssicher elektronisch signieren

Mit HIN Sign unterschreiben Sie mit Ihrer HIN Identität (eID) Dokumente einfach und sicher elektronisch. Die volldigitale und datenschutzkonforme Lösung schafft nicht nur Fälschungssicherheit, sondern spart auch Zeit und Kosten, die durch Ausdrucken und Postversand entstehen.

Für die Nutzung benötigen Sie einen HIN Anschluss mit einer persönlichen HIN eID. Für monatlich 5 Franken pro Anwender (HIN eID) können beliebig viele Dokumente signiert werden («Flatrate»). HIN Mitglieder haben die Möglichkeit, den Service unverbindlich zu testen. Auf sign.hin.ch können Sie die ersten zehn Dokumente gratis signieren.

Beweiswert nachträglich eingescannter Dokumente

Elektronische Beweisführung (eDiscovery)

Schweizerische Zivilprozessordnung
(Zivilprozessordnung, ZPO)

272

vom 19. Dezember 2008 (Stand am 1. Januar 2011)

---

3. Abschnitt: Urkunde

Art. 177 Begriff

Als Urkunden gelten Dokumente wie Schriftstücke, Zeichnungen, Pläne, Fotos, Filme, Tonaufzeichnungen, elektronische Dateien und dergleichen, die geeignet sind, rechtserhebliche Tatsachen zu beweisen.

Art. 178 Echtheit

Die Partei, die sich auf eine Urkunde beruft, hat deren Echtheit zu beweisen, sofern die Echtheit von der andern Partei bestritten wird; die Bestreitung muss ausreichend begründet werden.

Beweiswert

II. EINLEITUNG

II.2. STANDARDS und STAND DER TECHNIK

TR-RESISCAN 03138 „Rechtssicheres ersetzendes Scannen“
Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Technische, organisatorische und personellen Anforderungen an den Scanprozess und die möglichst rechtssichere Scanlösung
- Grundsätze des ordnungsgemässen Scannens

Beweiswert

III. MASSNAHMEN UND BEACHTUNGSPUNKTE

III.1. ZEITPUNKT DES SCANNENS

- Zeitpunkt des Scannens nachweislich und unabhängig von eigenen Zeitmessinfrastrukturen dokumentieren
- Elektronische Zeitstempel unabhängiger Anbieter von Zertifizierungsdiensten (Art. 2 lit. g ZertES) einsetzen
- Geschlossene, nicht manipulierbare Scan-to-Archiv Server verwenden
- Logdateien von RMS/DMS, sofern keine Manipulationsmöglichkeiten bestehen
- Scandateien ohne Zwischenspeicherung direkt in RMS integrierbar

Beweiswert

III. MASSNAHMEN UND BEACHTUNGSPUNKTE

III.3. FARBSCAN / SCHWARZ-WEISS-SCAN

- S/W-Bilddatei in der Regel ausreichend
- Hat Farbe eine qualifizierte rechtliche Bedeutung, Original mittels Farbscan digitalisieren

- Beweisrechtliche Relevanz der Originalfarbdarstellung abschätzen
- Negativliste oder Katalog von Dokumenten mit Farbscan festlegen
- Bei Auslagerung an Drittdienstleister sind klare Anforderungen zu definieren.

Beweiswert

III. MASSNAHMEN UND BEACHTUNGSPUNKTE

III.6. INTERNE QUALITÄTSSICHERUNGSMASSNAHMEN

- Massnahmen zur Sicherung der Qualität im Scanprozess
- Zentrales Mittel für Nachvollziehbarkeit der Entstehung und die Beweistauglichkeit eines Scanproduktes
- Sichtkontrollen
- Bei Massenverarbeitung: Stichprobenquoten auf Basis von statistischen Grundlagen
- Alle Massnahmen immer dokumentieren

- Momentaufnahmen mit Hauptzweck, systematische und wiederkehrende Fehler zu entdecken
- Zusätzliches Argument in der Argumentationskette zur richterlichen Überzeugung

Beweiswert

IV. SCHLUSSFOLGERUNGEN

- Ersetzendes Scannen führt zu einem Verlust des Beweiswertes, wenn anhand physischer Beschaffenheit (Merkmale) des Papieroriginals Beweis geführt werden muss. => Aufbewahrungspflicht

- Jeder relevante Inhalt lässt sich mit eingescannten Dokumenten rechtsgenüglich beweisen, wenn:
  - Scanning des Papieroriginals möglichst früh erfolgt
  - Auf einem geschlossenen, nicht von Dritten manipulierbaren Prozess beruht
  - Eine möglichst direkte manipulationsgeschützte Integration des Scanproduktes in das Zielsystem (RMS, DMS) stattfindet
  - Nachweisliche Verfahrensvorschriften des Scaningprozesses dokumentiert sind
  - Bekannte Standards und Normen angewendet werden
  - Qualitätssicherungsmassnahmen vorhanden und dokumentiert sind
  - Integritätsschutz durch Einsatz elektronischer Signaturen sichergestellt wird
  - Scanprozess allenfalls an Dritte ausgelagert wird (Manipulationsinteresse)
  - Freie Beweiswürdigung der Gerichte bleibt bestehen

Zusammenfassung

Zusammenfassung (1)

Aus juristischer Sicht bedarf es bezüglich des Umgangs **mit geschäftsrelevanten Informationen** im Unternehmen/öffentlichen Verwaltung einer umfassenden **Wahrnehmung** der **nicht übertragbaren Sorgfaltspflichten durch die Führungskräfte (VR und GL) (= digitale Leadership und digital compliance)**.

Führungskräfte haben die Vorgaben zu liefern (Records Management Policy)	**KOMMANDIEREN**
Sie haben die Einhaltung und Umsetzung zu	**KONTROLLIEREN**
Sie haben sich regelmässig – mindestens 1 x jährlich - über den Stand der Umsetzung und die Abweichungen zwischen IST und SOLL informieren zu lassen und die notwendigen Massnahmen zeitgerecht zu treffen. Massnahmen Sollten in einem Protokoll beweistauglich festgehalten werden.	**KORRIGIEREN**

Zusammenfassung (2)

Die Sorgfaltspflicht (Compliance) verlangt, dass die Führungskräfte **alle geschäftsrelevanten Informationen**

- **beweistauglich** und
- **revisionssicher**
- **jederzeit reproduzierbar**

erfassen (lassen) und **aufbewahren** (lassen).

www.fsdz.ch


Rechtsanwälte
ATTORNEYS @ LAW
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch
Impressum
Datenschutzbestimmungen
Profil
Kompetenzen
Team
Aktuell
Publikationen
Referenzen
Kontakt
Umsetzung der DSGVO
Hinweis schliessen
Als Anwaltskanzlei mit Schwerpunkt vor allem im Datenschutzrecht ist uns ein verantwortungsbewusster Umgang mit Ihren personenbezogenen Daten wichtig. FSDZ Rechtsanwälte & Notariat AG verzichtet vollständig auf den Einsatz von Social Media-Plugins, Websiteanalyse-Diensten und Anzeigen sowie Marketing-Diensten (keine Cookies, keine Google Analytics etc.). Sie können ohne Angabe von personenbezogenen Daten unsere Webseite besuchen.
FSDZ Rechtsanwälte & Notariat AG, Baar/Zug
Wir sind die Anwaltskanzlei für digitale Rechtsfragen mit den Schwerpunktgebieten
Informatikrecht,
IP-Recht (insbesondere Marken-, Urheber-, Lizenzrecht),
Cyberkriminalität und Forensik Computing,
Datenschutz und Datensicherheit,
Submissionsrecht im Informatik-Technologiebereich.
Ferner sind wir spezialisiert in den Bereichen
Europäisches E-Commerce-Recht für Onlineshops,
ICT-Security und Riskmanagement
Records Management und digitale Langzeitarchivierung sowie
Europäisches (DSGVO) und Schweizerisches Datenschutzrecht.
Jetzt anrufen 041 727 60 80
oder E-Mail schreiben
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Fax +41 41 727 60 85
sekretariat@fsdz.ch
Karte Google Maps
Rechtsanwalt
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch
Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch
Assoziierte selbständige Anwältin:
Eva Patroncini
Büro Uster
Imkerstasse 7
Postfach 1280
CH-8610 Uster
Telefon +41 44 380 85 85
patroncini@fsdz.ch
Partnerkanzlei de la cruz beranek Rechtsanwälte AG, Zug
de la cruz beranek Rechtsanwälte AG
Industriestrasse 7
CH 6300 Zug
Telefon: +41 41 710 28 50
Fax: +41 41 710 90 76
E-Mail: info@delacruzberanek.com
Website: >>>
Partnerkanzlei Lichtsteiner, Zug
Lichtsteiner Rechtsanwälte und Notare
Baarerstrasse 10
Postfach 7517
CH-6302 Zug
Telefon +41 41 726 90 00
Fax +41 41 726 90 05
info@llaw.ch
Website: >>>
Rechtsanwälte

Besten Dank

Lukas Fässler
Rechtsanwalt & Informatikexperte
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76B
6340 Baar / Zug
+41 41 727 60 80
www.fsdz.ch
faessler@fsdz.ch

Aufgabe

Formulieren Sie als Verwaltungsrat in maximal 3 Grundsätzen eine

Records Management Policy

für Ihr Unternehmen/Verwaltung.