PRIVACY & LAW FS 25

COMPLIANCE, RISK(MANAGEMENT), EU AI ACT & RECORDS MANAGEMENT

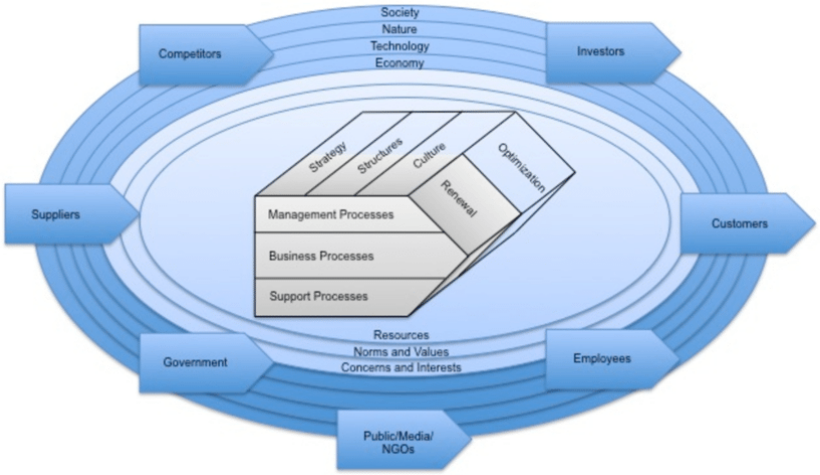
YOUR BENEFIT – AFTER THIS SESSION YOU KNOW…

1. Know the definition of „compliance“
2. Know the 5 key functions of compliance
3. Know the essentials of risk management
4. Know the essentials of the EU AI Act
5. Know the life cycle of records
6. Know the essential laws for records management


REQUIREMENTS
RULES
STANDARDS
GOVERNANCE
LAW
COMPLIANCE
POLICIES
TRANSPARENCY
REGULATIONS

WHY WE SPEAK ABOUT COMPLIANCE?

- A company as „**Productive Social System**" (St. Gallen Management-Model, 1972) is strongly embedded in a ecologic, economic and social (people, society, politic etc.) world. With each of them exists a connex, that has to be integrated. (is that a „biological" approach? Everything is connected with everything!?). Wiki: System Theory
- **Compliance as a part of the company culture**, communication, management, risk management and complying with external (law) and internal rules became the past 30 years more and more important.
- Personal Dataprotection Law is therefore not just a law - to comply with has a strong influence on (company-)culture, communication, risk-management and indeed - law.



DEFINITION OF COMPLIANCE

- **The term „compliance“ describes the ability to act according to an order, set of rules or request.**
  Compliance operates at two levels:
  Level 1 - compliance with **external rules** (e.g. **law, ISO-standards, Best Practices**) that are imposed upon an organisation as a whole.
  Level 2 - compliance with **internal systems** of control that are imposed to achieve compliance with the externally imposed rules.

COMPLIANCE ≠ CORPORATE GOVERNANCE

- Corporate Governance is a concept that covers a number of different aspects about the way in which an organisation is managed, directed and governed.

  It can be described as a set of relationships between a company's management, board, shareholders, and other stakeholders, which provides the structure through which the objectives of the company are set. Furthermore it provides the means of attaining and monitoring performance against those objectives.

- It's mainly „best practice" without direct legal consequence - but… (if the company goes bankrupt then the management will be measured by it!)

„SWISS CODE“ (of Best Practice for Corporate Governance)

- Introduced 2002 - actual version 2023, provided by economiesuisse and widely accepted by other organisations (even CH-Federal Government).
- *„Corporate governance encompasses all of the principles aimed at safeguarding sustainable company interests. While maintaining decision-making capability and efficiency at the highest level of a company, these principles are intended to guarantee* ***transparency*** *and a* ***healthy balance of management and control****.“*
- **Has an important role whether the CEO and Board of Directors acts professional or not**.

ISO 37301 – COMPLIANCE MANAGEMENT SYSTEMS (2021)

- **What is ISO 37301?**
  ISO 37301 is an international standard for compliance management systems (CMS). It provides guidelines for establishing, developing, implementing, evaluating, maintaining, and improving an effective and responsive compliance management system within organisations.

- **Why is ISO 37301 important?**
  ISO 37301 is crucial for organisations looking to ensure adherence to laws, regulations, and ethical standards within their operational context. It helps in mitigating risks, fostering a culture of integrity, and enhancing organisational governance and reputation.

- **Benefits of ISO 37301**
  - Promotes ethical business practices and reduces the risk of non-compliance
  - Enhances trust among stakeholders
  - Improves management processes and operational efficiency
  - Supports corporate governance and responsibility

COMPLIANCE: FIVE KEY FUNCTIONS

1. To identify the risks that an organisation faces and advise on them (**identification**)
2. To design and implement controls to protect an organisation from those risks (**prevention**)
3. To monitor and report on the effectiveness of those controls in the management of an organisations exposure to risks (**monitoring and detection**)
4. To resolve compliance difficulties as they occur (**resolution**)
5. To advise the business on rules and controls (**advisory**)

DEFINITION „RISK“

RISK = probability of incidence (%) x potential of damage (CHF)!

- Example: It’s very unlikely (%) that you get hit by a meteorite - but if so, it’s most likely letal (potential of damage).

- RISK is relative:
  - It happens twice a year that one of your customers can’t pay your invoice of ± CHF 30’000.– (but your yearly turnover is more than 1 Mio…)
  - The probability that our IT-system fails totally is 1% a year. If that happens the damage is estimated to CHF 50’000.– (insurance for that amount exists). But what’s your reputation worth?

RISK-MANAGEMENT: HANDLING THE UNKNOWN

„He who always does what he already can, always remains what he already is.“ (Henry Ford)

„Innovation starts in the mind with a bold idea and the courage to take risks.“

MOST IMPORTANT – TO IDENTIFY RISKS!

Looks like that the word „risk" is coming from the latin „resescum" - translated: „cliff"

- **Which risks?** Legally, technically, organisationally, financially, physically, personally etc. (**360° scope**)
- **Humans are risk factor #1!**
- **Do you have internal guidelines? Checklists?** Are they actual?
- **Do you know your main legal regulations?** Who is responsible? Are they actual?
- **Concern?** who is responsible?
- **Learn from faults!** Fail fast - learn fast!
- **International standards**: ISO 19600 (Compliance), ISO 15489 (Records Management), ISO 30302:2015 „Information and documentation – Management systems for records – Guidelines for implementation", ISO 27001 (Information Security), ISO 14000 (Environmental management), ISO Norm, „Gute-Labor-Praxis" etc. etc.

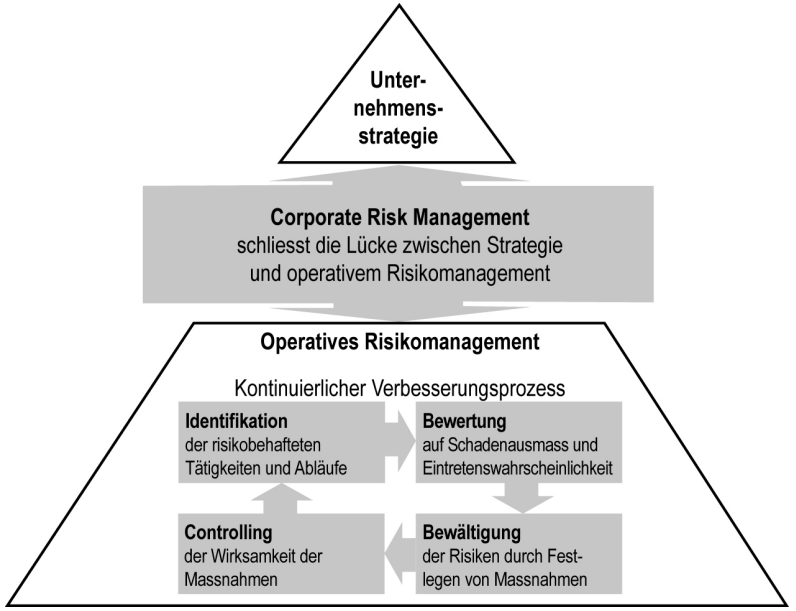
RISKMANAGEMENT: KNOW & HANDLE YOUR RISKS!

- „Climbing, Parachuting, Paragliding, Free-skiing, MX, Diving etc. are not dangerous per se - **dangerous is not to know its risks!**"
- **Analyse professionally your risks and decide the best strategy to handle the risks! Reevaluate!**
- Arrogance, proudness, ignorance, stupidity, greed are the most dangerous human factors!
  Thus being humble = security!
- **Attention to the „confirmation bias"!** What once went good doesn't have the next time!
- Attention to „peer pressure" (**Testosterone - not only in adolescence!**). Hierarchy („cockpit syndrome")!
- What's the best case / worst case scenario? **Define in advance clear limits to stop!**
- Trust is OK, but control is better!
- **Always watch/control the little things!**
- **Don't decide accidentally on mood! Make a rational decision based upon clear reasons! (useful: 6-thinking-hats-method from Edward de Bono)**
- **Have checklists!**
- **Learn & share your experience! Everybody is a risk-sensor!**

CLASSIC-TOP-DOWN-METHOD: CORPORATE & OPERATIVE RISKMANAGEMENT

Still useful in a rapidly changing world?

VUCA:
volatility
uncertainty
complexity
ambiguity



Source: www.kmu.admin.ch/kmu/de/home/praktisches-wissen/finanzielles/risikomanagement.html

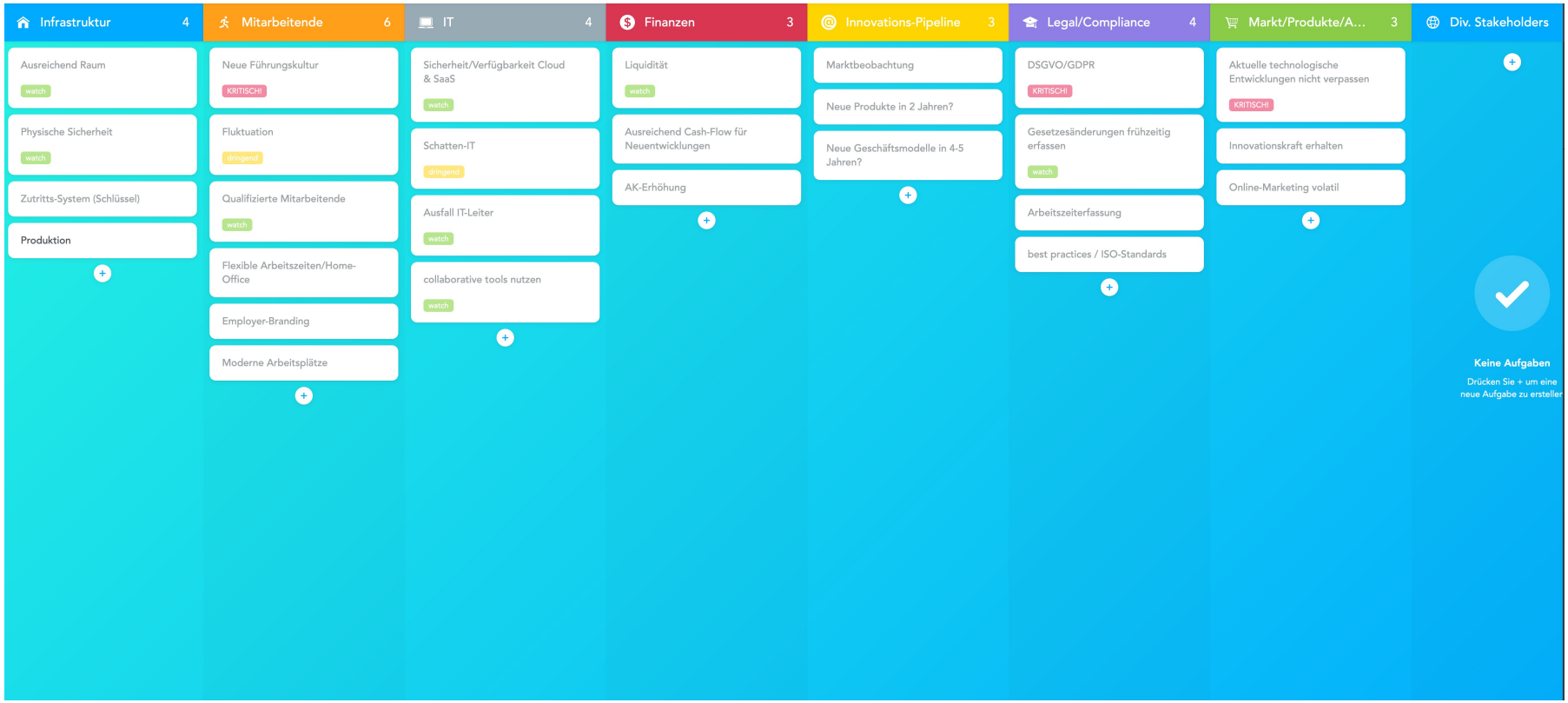
VUCA: Mainly a mind setting and constant reevaluation of the situation. Let different people participate to the risk-handling process! (1985, Bennis/Nanus)

360° VIEW OF RISKS

It's simple & obvious that „incidents" seldom have only limited effects. Thus it's important to recognise these effects as early as possible!

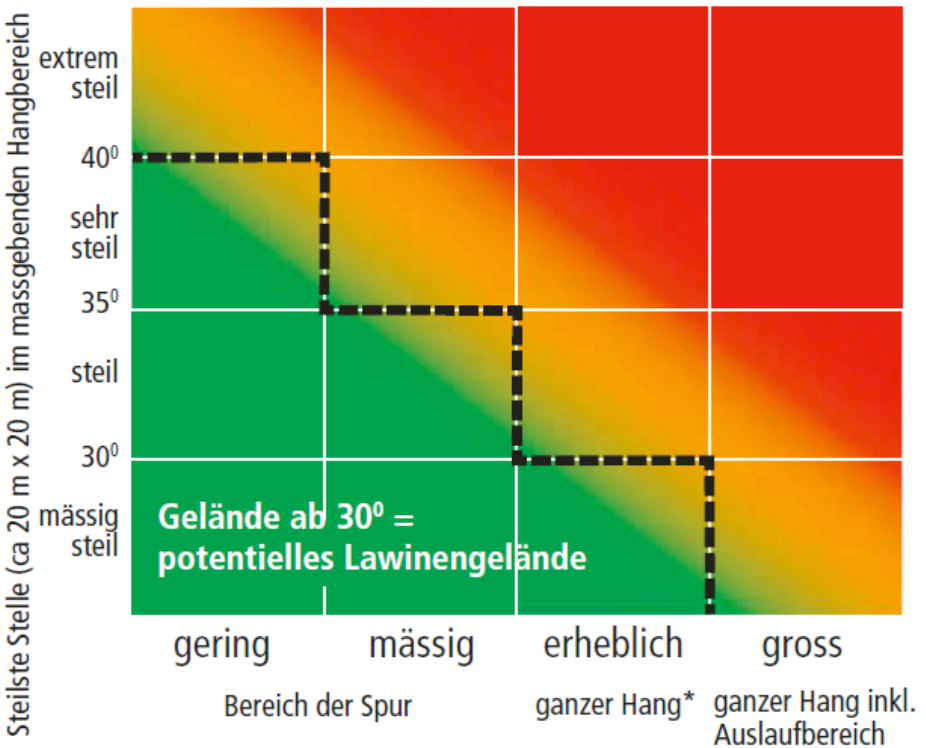
Attention! We're not talking about „crisis"! A crisis is an incident that hardly could be foreseen! Think about the „Black Swan" („not thinkable" incident with massive effect)

A BETTER 360°-MODEL: COLLABORATIVE RISK-MAP



With any Kanban-system (here Meistertask) you can establish such a rudimentary but useful risk-control-system.

MAKE RATIONAL DECISIONS UPON CLEAR REASONS...



Gefahrenstufen mit Hangbereich, wo die Hangneigung berücksichtigt wird.

Hohes Risiko
Verzicht empfohlen!

Erhöhtes Risiko, Vorsicht! Erfahrung!
- Lawinenproblem, ☺ ☹ abwägen mit Fokus auf das Lawinenrisiko im Einzelhang.
- Optimale Routenwahl und defensives Verhalten
- Risikomindernde Massnahmen
- Unerfahrene sollten diesen Bereich meiden
- Ausbildung und Erfahrung notwendig

Tiefes Risiko
Relativ sicher, wenn keine speziellen Gefahrenzeichen

Wenig Erfahrene bleiben besser unterhalb dieser Linie

* Falls es mit Argumenten begründbar ist, dass Fernauslösungen oder grössere Lawinen wenig wahrscheinlich sind (häufig bei: ständig befahrenen Varianten / Modetouren), muss bei erheblich nicht der ganze Hang berücksichtigt werden.

SLF: Avalanches & Prevention

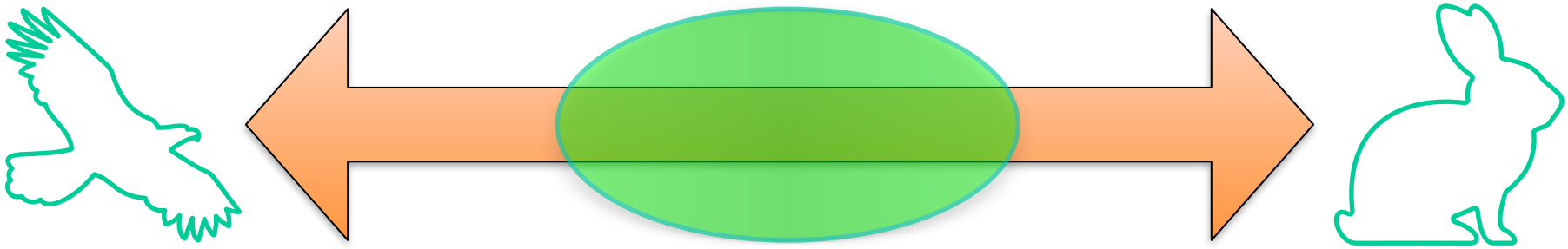
FIND THE RIGHT RISK CULTURE!

<u>There is no business without risks!</u>

If you avoid risks completely you will have no business!

Solution: constant awareness but flexible risk handling!

sweet spot



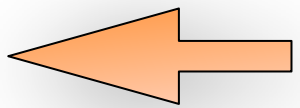
„there are no limits & rules for us“ (**stupid**)

„we have to fully comply with all rules & regulations“ (**stupid**)


The
EU
AI Act
Welcome to
the European Parliament

EU AI-ACT (1)

- Why EU AI-Act for Swiss Companies? Well - your customers might reside in the EU… (Art. 2 Abs. 1 lit. g AI Act)
  But as „simple" user the actual Swiss law knows no AI-specific restrictions - aside from potential data protection questions…
- The EU AI-Act is since 1th August, 2024 in power. Until 2nd August 2025 all EU-Member State has to designate and empower marked surveillance authorities.
- Useful: online EU AI Act Compliance Checker



EU AI-ACT (2)

- The AI-Act has a risk based approach:
  - AI systems for certain uses will be **prohibited**.
  - Certain AI systems will be designated as **high-risk AI systems** and subject to extensive obligations, especially for providers.
  - There will be specific provisions governing **general purpose** models. These models are regulated regardless of use case.
  - Other AI systems are considered low risk. These AI systems will be subject only to limited transparency obligations where they interact with individuals.

PROHIBITED AI SYSTEMS

- Certain AI systems for **biometric categorisation and identification**, including those for untargeted scraping of facial data from the internet.
- AI systems that deploy subliminal techniques, exploit vulnerabilities or manipulate human behaviour to circumvent fundamental rights or cause physical or psychological harm.
- AI systems for **emotion recognition** in law enforcement, border management, the workplace and education.
- AI systems for the **social scoring** evaluation or classification of natural persons or groups thereof over a period of time based on their social behaviour.

HIGH-RISK AI SYSTEMS

- AI systems used as safety components in the management and operation of essential public infrastructure e.g. **water, gas and electricity supplies**.
- AI systems used to determinate access to **education** institutions or in assessing students e.g. AI systems used to grade exams.
- AI systems used in **recruitment and employment** e.g. for placing job advertisements, scoring candidates or reviewing job applications, promotion or termination decisions or in reviewing work.
- AI systems used in migration, asylum and border control management or in various other **law enforcement** and judicial contexts.
- AI systems used for influencing the outcome of **democratic processes** or the voting behaviour of voters.
- AI systems used in the **insurance and banking** sectors.

The list of high-risk AI systems is not closed and may be supplemented in future as further high-risk uses for AI emerge.

DUTIES FOR PROVIDERS, DEPLOYERS, DISTRIBUTORS AND IMPORTERS OF HIGH-RISK AI SYSTEMS

- **Risk management system**: implementing process(es) for the entire lifecycle of the HRAIS to identify, analyse and mitigate risks.
- **Data and data governance measures**: training and testing of HRAIS must be undertaken in accordance with strict data governance measures.
- **Technical documentation**: drafting a comprehensive "manual" for HRAIS which contains specific minimum information.
- **Record-keeping**: HRAIS must be designed to ensure automatic logging of events including e.g. period of use, input data, and these must be kept by the providers for defined periods.
- **Transparency**: HRAIS must be accompanied by instructions for use which include detailed information regarding their characteristics, capabilities and limitations.
- **Human oversight**: HRAIS must be designed so they can be overseen by humans, who should meet various requirements e.g. being able to understand the HRAIS ('AI literacy') and to stop its use.
- **Accuracy, robustness and cybersecurity**: HRAIS must be accurate (with accuracy metrics included in instructions for use), resilient to errors or inconsistencies (e.g. through fail-safe plans) and resilient to cyber-attacks.
- **Quality management system**: HRAIS providers must put in place a comprehensive quality management system.
- **Post-market monitoring**: HRAIS providers must document a system to collect and analyse data provided by users on the performance of the HRAIS throughout its lifetime.
- **CE marking**: Providers must ensure their HRAIS undergoes a conformity assessment procedure before the HRAIS is supplied and affix a CE mark to its documentation.
- **Registration in EU database**: Providers and public bodies using HRAIS must register the HRAIS in an EU-wide database of AI systems.
- **Reporting obligations**: HRAIS providers must report serious incidents or malfunctioning involving their HRAIS to a relevant authority within 15 days.

GENERAL PURPOSE AI SYSTEMS

- AI technologies which are not prohibited or high-risk are subject to much less onerous regulatory requirements.
- The most onerous other requirements under the AIA attach to **general purpose AI** (GPAI). The requirements for most GPAI models, which includes foundation models and generative AI models, are chiefly focused on transparency.
- The obligations for all GPAI include issuing technical documentation, compliance with EU copyright law and providing summaries of the training data.
- The EU AI Act includes additional requirements for GPAI that is trained on extensive data sets and exhibits superior performance; this is based on the potential systemic risks that these AI models may pose across the value chain (**GPAI with systemic risk**).
- Any GPAI model with systemic risk will be subject to additional requirements that are expected to include:
  - Stringent **model evaluation**s, including adversarial testing/red-teaming.
  - Assessing and mitigating possible systemic risks from use of the GPAI.
  - Greater **reporting obligations** to regulators, particularly where serious incidents occur.
  - Ensuring adequate **cybersecurity** for the GPAI with systemic risk.
  - Reporting on the **energy efficiency** of the GPAI.

RECORDS MANAGEMENT (ISO 15489)

LIFE CYCLE OF INFORMATION/RECORDS

Migration?

RECORDS MANAGEMENT – BEST PRACTICES & LEGAL REQUIREMENTS

Standards & best practices:

- ISO 15489 (Records management 2016)
- ISO 19005-1:2005 (Document management - Electronic document file format for long-term preservation/PDF-A)
- ISACA
- COBIT
- Treuhand-Kammer
- BS 7799/ISO 17799
- Good Laboratory Praxis (GLP)
- and others

Laws:

- 957 ff OR
- GeBüV
- MWST (VAT)
- ZPO
- ATSG
- revDSG/DSV
- and others

MOST IMPORTANT: CATEGORISE!

- You don’t have to treat all records the same!
- You have to give any record a **metadata** (date of issue, change, owner, rights of use, expiry etc.) and treat them differently! Full-text retrieve is not sufficient!
- Safekeeping periods (begins on expiry of the financial year!): **5 or 10 years**, but: you’re not forced to delete/ destroy on the first day after the deadline…

CRIMINALLY LIABLE

- *„Any debtor who fails to comply with a statutory obligation to which he is subject to keep and preserve business accounts or draw up a balance sheet, with the result that his financial position is not or not fully ascertainable, is liable, if bankruptcy proceedings are commenced against him or a certificate of unsatisfied claims has been issued in his respect following a seizure of assets in accordance with Article 43 DEBA (SchKG), to a custodial sentence not exceeding three years or to a monetary penalty.“* (**Art. 166 StGB**).
- *„Any person who wilfully or through negligence fails to comply with the statutory duty to keep proper accounts or to preserve accounts, business correspondence and business telegrams, any person who wilfully or through negligence fails to comply with the statutory duty to preserve accounts, business correspondence and business telegrams, is liable to a fine.“* (**Art. 325 StGB**)

RESPONSIBILITY OF THE BOARD OF DIRECTORS (VR)

Art. 754 OR

1 The members of the board of directors and all persons engaged in the business management or liquidation of the company are liable both to the company and to the individual shareholders and creditors for any losses or damage arising from any intentional or negligent breach of their duties.

2 A person who, as authorised, delegates the performance of a task to another governing officer is liable for any losses caused by such officer unless he can prove that he acted with all due diligence when selecting, instructing and supervising him.

KEEPING AND RETAINING ACCOUNTING RECORDS

Art. 958f OR

1 The accounting records and the accounting vouchers together with the annual report and the audit report must be retained ***for ten years****. The retention period begins on expiry of the financial year.*

2 The annual report and the audit report must be retained in a written form and signed.

3 The accounting records and the accounting vouchers may be retained on paper, electronically or in a comparable manner, provided that correspondence with the underlying business transactions and circumstances is guaranteed thereby and provided they can be made readable again at any time.

4 The Federal Council shall issue regulations on the accounting records that must be kept, the principles for keeping and retaining them and on the information carriers that may be used.

DECREE OVER THE KEEPING AND ARCHIVING OF BUSINESS RECORDS – ART. 2 II GeBüV

2 If the books of account are kept and preserved electronically or in a comparable manner and the accounting documents are recorded and preserved electronically or in a comparable manner, ***the principles of proper data processing must be observed****.*

INTEGRITY (AUTHENTICITY & UNALTERABILITY – ART. 3 GeBüV

The accounts must be kept and retained in such a way and the supporting documents must be recorded and retained in such a way that they cannot be altered without it being possible to establish that they have been altered.

DOCUMENTATION DUTIES – ART. 4 GeBüV

1 Depending on the nature and extent of the business, the organisation, responsibilities, processes and procedures and infrastructure (machinery and programmes) used in the maintenance and safekeeping of accounts shall be documented in work instructions in such a way that the accounts and accounting records can be understood.

2 Work instructions shall be updated and retained in accordance with the same principles and for the same length of time as the books of account kept thereafter.

FURTHER DUTIES FROM THE GeBüV

- General duties of care (Art. 5 GeBüV)
- Availability (Art. 6 GeBüV)
- **Separation of useful data from archive data** (Art. 7 GeBüV)
- **Organization of archive data** (Art. 8 GeBüV)
- Media and Migration (Art. 9 & 10 GeBüV)

OBLIGATION TO PROVIDE PHYSICAL PROTECTION

Art. 3 DSV (2023):

„1 Um die Vertraulichkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

*a. berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (**Zugriffskontrolle**);*

*b. nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (**Zugangskontrolle**);*

*c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (**Benutzerkontrolle**).*

2 Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

*a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (**Datenträgerkontrolle**);*

*b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (**Speicherkontrolle**);*

*c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (**Transportkontrolle**);*

*d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (**Wiederherstellung**);*

*e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (**Zuverlässigkeit**) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**)*

*f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (**Systemsicherheit**).“*


Take away