

Confidence in your business procedures and information

Information governance
Electronic archiving

May 2018





Introduction

Data and information are not only a part of our everyday life, for many businesses and organisations they are essential to survival. This is either because businesses fundamentally generate their income with data, develop products and services, ensure smooth-running and efficient operations or manage their risks and compliance with legal and regulatory requirements through reliable data. Ongoing digitisation increases the flood of information even more, and requires effective methods to stay in control of the important data and ensure it's managed according to requirements.

A strategic management of information ensures that you can create added value and utilise and process data efficiently throughout its whole life-cycle. All this forms part of an effective Information Governance. When it comes to important data and information, their authenticity, integrity and reliability should be maintained throughout their whole life-cycle. Only then can the information retain its value in the long term, and can also be used as evidence. This requires compliant electronic archiving. Further, electronic archiving combined with an effective Information Governance form the basis for digitalisation.

In the following guide we will show you how you can bring your electronic archiving up to date, while also implementing basic Information Governance. These instructions apply to every company based in Switzerland or with a Swiss VAT number.

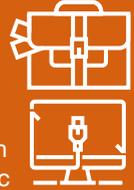
In what follows we refer to books of account and accounting records as “information to be archived”.

Good to know:

Electronic versus hard copy

On principle all information may be stored in electronic form, although certain documents must be kept as originals regardless of their form. The company should therefore carry out a risk analysis of the documents, and based on that decide which information is still to be stored in physical form as before, and which is to be stored only in electronic form. For example, the Swiss Federal Tax Administration (FTA) points out that electronic and physical documents can have the same evidentiary value, provided the requirements for electronic archiving are complied with. Ultimately the burden of proof, proving the existence of an alleged fact, rests on the person who derives rights from that fact. (Swiss Civil Code, Art. 8). The evidential value of digitised information can be substantially secured by applying appropriate controls (ICS) in the processes and IT systems.

The solution design documentation is required by law, and further supports the probative value of electronic information.



Business objectives form the basis

To ensure that your data and information supports your organisation in the best possible way, you should ask yourself the following questions:

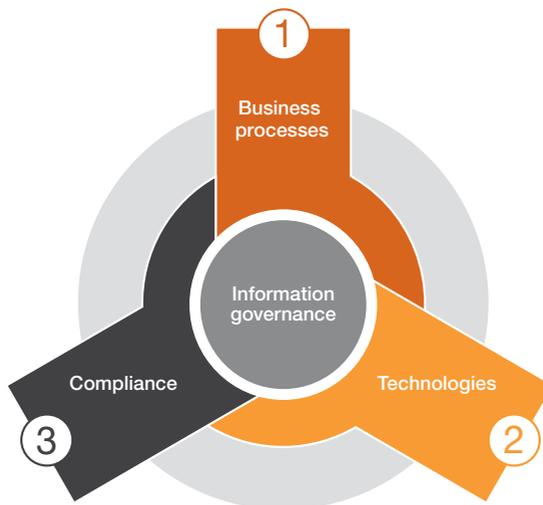
- What are the requirements of our clients, and of our organisation, and how do we wish to manage and use information in the future?
- How can information help us to achieve our business objectives, and what level of data availability, quality, integrity and security do we need?
- How can we ensure that we comply with laws and industry standards?
- What resources and partners do we need to implement our vision in practice?
- How can we make sure that the investments in IT and data projects achieve the desired result?

These are all questions which you should ask as part of your information strategy, and then initiate appropriate measures and define measurable key performance indicators.

For this, you should also ask from the operational standpoint which business processes you want to automate and which information you would like to digitise. This way you will reduce the costs for administration, filing and searches, minimise risks, and the staff can focus more on activities which create added value.

Depending on your goals, you should find an appropriate balance between risk, protection and security, and the use and distribution of information.

A coherent management of business information rests on three pillars.



Central to it all: your Information Governance

Successful management of business information is based on the interplay between technologies, business processes and compliance (see illustration). To harmonise the relevant areas of your organisation, a number of challenges have to be mastered. It requires commitment, a change in understanding, and a cultural change regarding the way information is managed.

To master the various challenges and successfully use, manage, archive and delete information, you need an organisational structure, principles, rules and methods which make this possible. You need Information Governance.

The life-cycle of information can be seen as an iterative process.



Where does your company stand when it comes to archiving?

Nowadays electronic archiving is more than just an isolated data storage medium, which stores information for a certain period of time. Electronic archiving provides confidence that you can rely on the content of the information. Even in the age of automation, distributed systems and (e.g. cloud computing) machine learning, it provides traceability and trust.

What is more, archived information is being increasingly integrated into operational business procedures.

Your company should have an understanding of the organisational and technical requirements of archiving. The following basic questions will help you in achieving this:

- Who are our stakeholders with interest in our archived business information?
- Which business documents and data should/must we keep (in what form, for what reasons, for how long)?
- What requirements does the electronic archive need to meet in terms of confidentiality, security and compliance?
- How do we ensure the availability, integrity and readability of the archived information technology?
- How does our electronic archive support our business processes and projects in the area of data and information?
- Which service providers and technologies do we use for archiving?

Good to know:

Archiving abroad



Storage in another country is permitted – provided one complies with the said Swiss regulations (especially those concerning data protection), and the documentary evidence is accessible from Switzerland within a reasonable time. Special attention should be paid to the archiving solution and outsourcing partner in the other country, they should in any case confirm that they comply with Swiss law.

If data and information from abroad are to be archived in Switzerland, note that this archived information is subject to the storage regulations of the country of origin. In such cases it is recommended that you consult an expert – where possible a local one – about the requirements of storing this information in Switzerland.

The data catalogue as a practical helper

The data catalogue is an index and also an effective tool for recording and classifying the important data elements and documents. If you want to manage information efficiently throughout the whole life-cycle, it is crucial that you know what data you hold, how it is handled and potentially even how it was gathered (e.g. data privacy laws). This data catalogue can also be created, automated and updated with the aid of modern technology.

The best way for you to keep an overview of the various different storage periods for your business documents is by producing a data catalogue, filing plan or retention schedule, as appropriate.

In short, this will typically include the following details about storage and retention of data:

- List of the relevant data/information (business documents)
- Participating systems according to the information architecture over the whole information life-cycle
- Allocated responsibilities and contact persons
- The relevant legal framework
- The required retention period (stating the initial trigger to start the retention period)
- What actions are to be carried out when the period ends (e.g. deletion process)
- Location if stored as hard copy, or target system if stored electronically
- Any dependencies of the data/information and other classifying features

Good to know:

Data migration



When carrying out a data migration you have to keep a record and logs of the transfer from one information carrier to another. You have to retain these records and logs along with the migrated information. Additionally, a suitable control environment must be set up during the data migration which at least covers the following aspects:

- Completeness and accuracy
- Continuing availability and readability of the migrated information

To document a data migration in compliance with the regulations, we recommend that you prepare a migration concept and plan. Another point to note is that due to the very short IT innovation cycles, migrations are usually carried out approximately every five years.



Solution Design documentation of procedures as a mandatory action

You have to document the digital procedures and electronic archiving in your company when handling crucial business information, this is required by the Ordinance on Maintenance and Retention of Accounts (GeBüV, Art. 4).

This solution design documentation provides an expert third party with the context they need to understand the management of your books of account and archived information as quickly as possible, from your organisation, processes, procedures and infrastructure (systems and programs). The solution design documentation must be retained along with the information itself.

Here are some examples of the content:

- **Legal requirements:** Which legal requirements are relevant to your company? Are there any special industry-specific requirements?
 - **Requirements that are not process-specific:** Who is responsible for the area of information processing and who owns the data? Does your environment meet the business requirements for disaster recovery?
 - **Processes:** What are the relevant information and workflows? Which actions do you perform manually, and what are the automated processing steps? How is traceability ensured?
 - **IT:** Who is the manufacturer of your application program? Which version/configuration do you use? How are the interfaces to other systems setup?
- **Quality:** What checks do you do manually, and which ones are automated (e.g. compare amounts, check master data etc.)? How do you ensure the integrity of your information? How do you verify that the information is complete? Are these checks part of the formal internal control system (ICS)?

Good to know:

Attestation versus certification



Various solution providers for electronic archiving offer certifications for their software.

A certification basically shows that the software can meet the legal requirements when used properly. A software certification is not sufficient, however, to completely guarantee the probative value of electronic information, one reason being that such certificates refer to the IT systems only but not the organisational and procedural controls in the organisation. To provide a comprehensive warranty, you can seek an attestation by an independent third party, which takes into account the specific corporate environment. Such an attestation also has the advantage that it can refer to the whole life-cycle of the information, and thus provides a more far-reaching guarantee of evidentiary value than a software certification.

Legal framework

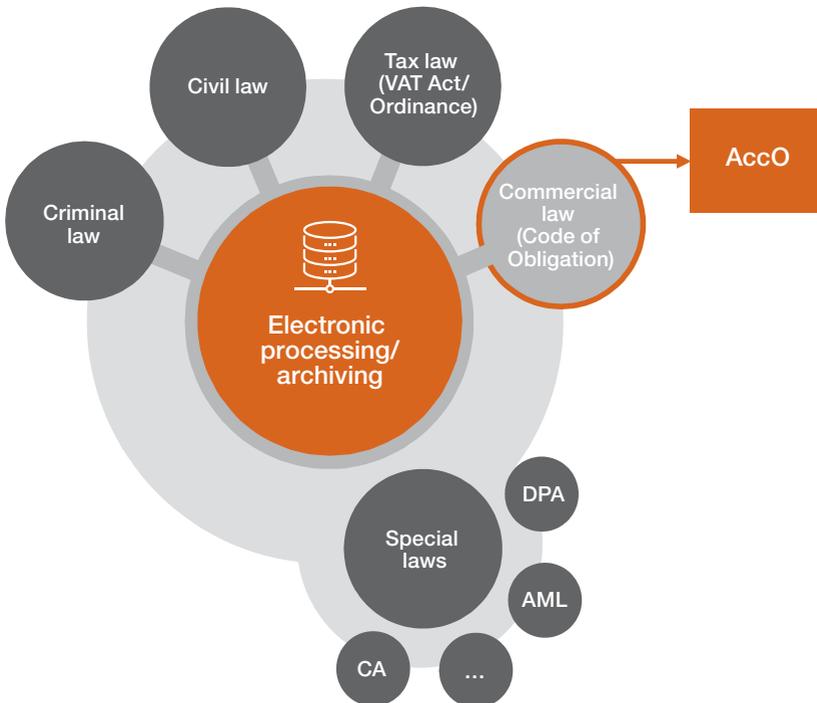
Commercial tax and data protection law

Basically you have to retain your information to be archived, for a period of ten years from the end of the financial year. There are, however, different variations on, which you need to model in your solution. For business documents concerning real estate the retention period is twenty years, according to the Swiss VAT Act. For customs-related records, retention periods vary from three months to five years. Finally, from a data privacy perspective, you need to be able to delete certain information about individuals.

There are also specific industry regulations and limitation periods to be observed, which can sometimes be longer than the actual (minimum) retention periods.

Besides the legal requirements, risk considerations may suggest additional information to be retained or other storage periods.

The regulations can vary widely and should be considered individually for each organisation.



Good to know:

Digitalisation: the example of invoices



If the invoices are now only being sent and exchanged in electronic form (for example by e-mail), the provisions of the VAT Act and the Ordinance on the Maintenance and Retention of Accounts apply. It is important to have an appropriate control environment for the processing of e-invoices in order to avoid significant input tax deduction losses.

You will find more about this topic in our brochure **“Electronic Invoicing”**.

Special legal provisions



The provisions of the Code of Obligations provide the basic norms for accounting and the archiving of business information in Switzerland. In addition to this, there are also various special provisions in other areas of the law which have to be observed. Customs Act (CA), for example, regulates the retention of documents which serve as evidence when tracking customs administration (DPA). The Data Protection Act is particularly important for such areas as the processing and archiving of personally identifiable data on servers in Switzerland and abroad, and the cooperation with external service providers (outsourcing) and partners. The Money Laundering Act contains special rules for financial intermediaries regarding the retention of documents. Then there is the Casino Act, for example, which has provisions on the storage of certain types of information. There are also industry-specific requirements which apply in some way to archiving, such as the provisions of the Swiss Financial Market Supervisory Authority (FINMA) concerning specific areas (such as digital client on-boarding, securities trading, outsourcing, market rules of conduct, etc.); there is also Good Manufacturing Practice (GMP) in the area of life sciences.

The legal basis for electronic archiving is commercial law. The provisions on commercial accounting (Art. 958f Swiss Code of Obligations) allow companies that are required to keep accounts to store their books of account and accounting records electronically under certain conditions.

Ordinance on the Maintenance and Retention of Accounts

The Ordinance (Acco, GeBüV) and Maintenance and Retention of Accounts sets out the detailed provisions for electronic archiving. It covers the following areas:

Ensuring integrity, and selecting a permitted information carrier

- You have to manage and store your archive information in such a way that it cannot be modified without the changes being detectable (GeBüV, Art. 9).

The following information carriers can be used for archiving:

- Uneditable information carriers such as paper, image media, WORM (write once read many) storage devices, CD-R, DVD-R and UDO (ultra density optical), or
- Editable information carriers such as magnetic tapes, magnetic or magneto-optic diskettes, internal or removable hard drives and solid-state memories.

Editable information carriers are, moreover, only permitted if a) the integrity of the stored information is ensured by technical methods (e.g. digital signature, special WORM software); b) the time when the information was saved can be shown unalterably (e.g. by a time stamp) and c) the procedures, methods and their use are documented (see page 9), and relevant supporting information such as protocols and log files have also been retained.



Finally, it should be noted that not all permitted archive media are equally suitable in practical terms for long-term archiving. For example, DVDs often become unreadable after just a few years, so readability checks and migration to different media have to be done much more frequently than for other media. There is also a greater risk of an irreversible loss of data.

Ensuring the protection of archived information

You have to store the information that is to be archived carefully, arranged in an orderly fashion, and protected against harmful outside influences (Company Accounts Ordinance, Art. 5). These requirements can be managed as part of a “disaster recovery plan” (including backup). You also have to safeguard the archived information against unauthorised access, and log and keep a record of when it is accessed.

Ensuring availability

You have to store the archived information in such a way that it can be viewed within a reasonable time (5 to 10 working days in the case of physical archiving, a few minutes in the case of electronic archiving); the same applies to the tools needed for this (Company Accounts Ordinance, Art. 6). Moreover the archived information must also be viewable without having to use special tools. Therefore it is recommended that the information that is to be archived should be kept in readable storage formats suitable for archiving purposes.

Archived information is to be kept separate from operational information, or designated as such (Company Accounts Ordinance, Art. 7).

Regular inspections

You have a duty to regularly check the integrity and readability of the information carriers and archived information. This can be done with the help of manual or automatic controls.

Good to know:

Consequences of non-compliance



The violation of archiving regulations can have significant financial consequences due to the legal and tax regulations. A concrete example: For input tax deduction, properly stored digitised input statements are still the simplest and most effective way to secure the input tax deduction, even though one has a free choice of documentary evidence. In the case of non-compliance one risks financial damages depending on the level of revenues involved, and a fine. Sanctions or fines may also be imposed if there is a breach of industry-specific archiving regulations.



Click for more details

You will find more information on the topic of electronic archiving and more law texts here:



Further principles

Brochure

“Electronic Invoicing”

A Guide for Companies and Institutions

Translated for you

Download the **Company Accounts Ordinance (GeBüV)** in English.

Further information

www.pwc.ch/en/services/risk-assurance/information-governance.html

Legal framework

Swiss Code of Obligations (OR , in German), SR No. 220

Ordinance on the Maintenance and Retention of Accounts (GeBüV, in German), SR No. 221.431

Federal Act on Value Added Tax (VAT Act, MWSTG in German), SR No. 641.20

Swiss Federal Act on Data Protection (DSG in German, in German), SR No. 235.1

Customs Act (ZG, in German), SR No. 631.0

Discuss further

Ralf Hofstetter

Information Governance
+41 58 792 56 25
ralf.hofstetter@pwc.ch



Jochen Richner

Tax Technology Solutions
+41 58 792 57 55
jochen.richner@pwc.ch

Susanne Hofmann

Legal Compliance & Data Protection
+41 58 792 17 12
susanne.hofmann@pwc.ch

