Swiss Banking

Cloud Guidelines

November 2025
Guidelines of the SBA
3rd edition

Contents

Note:
Changes from the second edition are marked with an asterisk (*) in the legal and regulatory guidelines and listed at the end of the document. Minor changes with no material impact are not marked.

Foreword

The digital transformation in the financial sector is moving forward inexorably, causing the importance of cloud services for the sector to grow. In this third edition of the Swiss Bankers Association (SBA) Cloud Guidelines, we discuss developments and challenges with regard to the use of cloud technology by banks and securities firms.

New technologies are helping to make the Swiss financial sector more competitive: depending on the situation, cloud services can improve efficiency and security while reducing costs as well as providing scope to develop innovative services and bring them to market quickly and flexibly. At the same time, the resilience of banks' and securities firms' infrastructure and the trust people place in their ability to function play a key role. However, cloud services can also give rise to risks such as a possible dependence on third parties, and failure to use them correctly can result in a loss of control.

Regardless of the technology employed, legal and regulatory requirements apply. In particular, professional confidentiality under the Banking Act and Financial Institutions Act must be maintained, and compliance with data protection law as well as data security and resilience must be assured, for example in connection with critical data as set out in the Swiss Financial Market Supervisory Authority FINMA's Circular 2023/01 "Operational risks and resilience – banks".

Interpreting these requirements – and in particular implementing them by means of appropriate technical and organisational measures (TOMs) – can be more or less of a challenge, depending on the business and operating model involved. A working group headed by the SBA thus drew up a set of legal and regulatory guidelines (hereinafter referred to as the guidelines) for the use of cloud services by banks and securities firms in 2019. These guidelines contain recommendations for institutions on the procurement and use of cloud services.

The Cloud Guidelines have been updated to take account of the legal and regulatory developments that have occurred since they were first published, for example in the regulations on operational risks.

The guidelines are divided into two parts. The first contains a general introduction to the topic of the cloud. It identifies the benefits and advantages of cloud technology for banks and securities firms and sheds light on what the SBA sees as sensible principles as well as the key regulatory issues relating to the use of cloud services by banks and securities firms and sets out the SBA's solution approaches. The second part contains legal and regulatory recommendations from the SBA with reference to Swiss law.

Another key aspect in connection with the use of cloud services by banks and securities firms is defining and implementing appropriate technical and organisational measures to specify and operationalise the business policy and legal requirements concerning the use of cloud technology. Each institution must tackle this challenge for itself in line with its own specific use case.

This document does not claim to cover all eventualities. It will be updated and revised regularly to take account of future developments in technology and the law. The current version will be published.

Management summary

- The **use of cloud technology** is a **critical success factor** for Switzerland and its financial centre. A clear understanding of the legal and regulatory requirements for banks and securities firms and the ability to develop and implement appropriate technical and organisational measures to ensure that they are met are essential.
- This document comprises a set of legally **non-binding guidelines** as an aid to interpretation in practice for institutions procuring and using cloud services. It focuses on four areas:
  - **Governance (including risk management):** choosing the cloud provider and its suppliers (subcontractors), consent to a change of supplier
  - **Data processing:** processing bank client data
  - **Authorities and proceedings:** transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts
  - **Audit:** auditing the cloud services and the cloud infrastructure used to deliver them
- The guidelines show institutions practicable solution approaches for the most important legal and regulatory requirements. The most vital aspect of cloud use, namely assessing the **risks** and defining appropriate technical and organisational measures to deal with them, remains **the responsibility of individual institutions.**

Cloud services in practice

Benefits and advantages of cloud services

The digital transformation in the financial sector is moving forward inexorably, causing the importance of cloud services for the sector to grow. Depending on the situation, cloud services can improve efficiency while reducing costs as well as providing scope to develop innovative services and bring them to market quickly and flexibly. Some specialised cloud providers also offer enhanced security for banks and securities firms. As such, cloud services are a critical success factor for the Swiss financial centre.

Many clients use cloud services in their everyday lives without necessarily knowing that they are doing so, for example when they send e-mails, stream music and films or save their holiday photos in the cloud. What works in the private sphere should also be possible for highly specialised institutions and their complex business. Regardless of the technology employed, however, legal and regulatory requirements apply.

Migrating infrastructure and processes to a cloud can often reduce the time it takes for institutions to bring innovative products and services to the market and thus increase their competitiveness. The cloud enables banks to exploit new technologies such as artificial intelligence without making substantial investments in their own hardware and software. Access to a large pool of data and the corresponding computing power allows large data volumes to be analysed in real time, enabling banks to offer innovative, tailor-made advisory services to individual clients or automate complex compliance and risk processes. The cloud also permits substantial efficiency gains in the development and testing of new applications and systems: innovative ideas can be piloted simply and flexibly, explored in more depth or abandoned, and therefore realised more easily. Finally, the range of functions offered by cloud services can in principle be used at variable cost levels on a self-service basis. Since institutions only have to pay for the services they directly use, they can, for example, react more flexibly to fluctuations in demand by switching IT resources on or off.

There is no longer a need to build up or buy in the skills and resources needed to operate an in-house IT infrastructure, making the use of cloud services a particularly attractive proposition for small institutions. Technologies that used to be restricted to large companies will also become accessible to small ones and enable significant economies of scale.[1] However, new skills must be built up and optimised to ensure that cloud services are managed and steered efficiently and effectively. Using the cloud also makes it easier to meet the growing demands placed on IT operations (IT security, keeping up to date with patches[2], managing the IT infrastructure lifecycle).

Swiss institutions are becoming increasingly aware of the use of cloud services. At the same time, a welcome degree of competition has opened up between national and international cloud providers. The increasing exploitation of cloud services will further strengthen Switzerland's financial centre and financial ecosystem in the future.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud can be used in three models – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) – and supplied in four different ways – private cloud, community cloud, public cloud and hybrid cloud.[3]

1 A marginal cost equation indicates that many institutions cannot set up a cloud of their own at the same costs as specialised cloud providers. The cloud allows IT resources to be turned on or off as required and thus matched precisely to the fluctuating demands of business activity.

2 A small piece of code that repairs errors in (mostly large) application programs.

3 Definition according to NIST (2011): https://csrc.nist.gov/publications/detail/sp/800-145/final.

Fundamental considerations on the use of cloud services

Depending on the institution's specific business and operating models as well as its strategy, the first step should be to determine concrete business policy goals for the use of cloud services. As a second step, institutions are advised to identify and interpret the relevant legal and regulatory requirements. Both should then be translated into internal requirements, including requirements for technical and organisational measures[4] used to select, employ and monitor cloud services.[5] These requirements are typically implemented as part of institution-wide cloud projects involving a large number of stakeholders and a broad division of labour. Binding governance with clear tasks, authorities and responsibilities (including controls) ensures correct operation after the project is completed.

In summary, selecting, procuring and operating cloud services is a process that involves a broad division of labour as well as a large number of business policy, institution-specific and external constraints.

From a legal perspective, the focus is on managing service providers, with the applicable legal and regulatory requirements depending in particular on the institution's target operating model, the cloud provider's characteristics, the type of data involved and the location at which they are processed, including access for maintenance purposes, for instance. In principle, the more sensitive the data involved and the greater the extent to which they are processed abroad, the stricter the requirements.

Cloud providers must generally comply with the same requirements as the institutions they serve and must therefore be contractually obliged to do so. This means that the institution's data organisation must be sufficiently mature, including data and risk governance and their granular control, and the cloud provider must be sufficiently flexible.

Key approaches from the SBA in the guidelines

These guidelines, without reference to any legal or regulatory obligations, contain legally non-binding recommendations for institutions procuring and using cloud services as well as interpretations of the legal bases applicable to cloud services. They focus on four areas:

- **Governance (including risk management):** choosing the cloud provider and its suppliers (subcontractors), consent to a change of supplier
- **Data processing:** processing bank client data
- **Authorities and procedures:** transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts
- **Audit:** auditing cloud services and the cloud infrastructure used to deliver them

4 Defining and implementing appropriate technical and organisational measures is not a legal issue.

5 This is expressly reflected with regard to personal data, for example, in Art. 7 para. 2 of the revised Federal Act on Data Protection (FADP).

The guidelines show practicable solution approaches for the regulatory requirements. The SBA has thus taken on an important task for the benefit of the Swiss financial centre. When applying the guidelines, however, institutions should adopt a risk-based and proportionate approach that reflects their size as well as the complexity, structure and processes of their business model.

A) Choosing and changing cloud providers and subcontractors[6]

Purpose of the recommendations set out in the guidelines:
The institution should, **at all times, have the most important information it needs to select a cloud provider,** taking account of its significant subcontractors.

Cloud providers take advantage of the opportunity to define and change the operating models, the technologies used, service providers within and outside the group, and other essential factors, with a view to efficient and competitive service delivery (design authority).

When choosing a cloud provider, therefore, the following points in particular need to be considered:

- ability to fulfil contractual obligations, in particular by means of appropriate technical and organisational measures;
- financial stability;
- legal system to which the provider is subject.

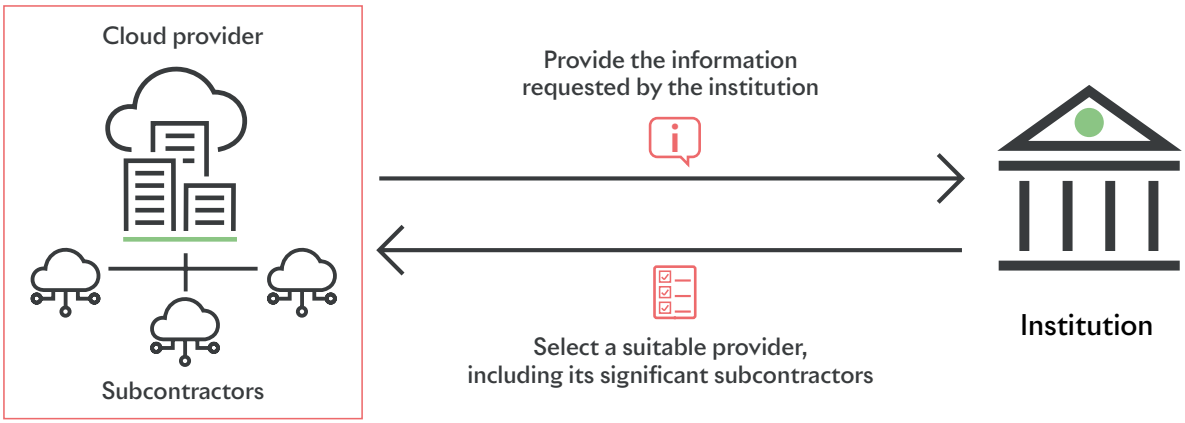
The institution should also establish whether, in addition to these performance-related criteria, the cloud provider is able to assume the essential contractual duties arising out of financial market and data protection legislation and fulfil these by means of technical and organisational measures.

6 See also chapter II:5 of the guidelines.

Figure 1

Choosing and changing providers and subcontractors

Providers' duties towards the institution



The cloud provider should provide the institution with the information it requests and has to notify it of any significant subcontractor. If the institution does not agree to this, it may terminate its contract with the cloud provider and recover the functions, services and any bank client data that have been outsourced, or transfer them to new cloud providers.

Source: Swiss Bankers Association (SBA) 2025

When choosing a cloud provider and its subcontractors, high priority must be attached to the security of the data (i.e. confidentiality, integrity, availability and traceability) as an integral part of the underlying due diligence.

The institution should in particular be informed in advance of a change of significant subcontractor (see Figure 1).[7] It should also take suitable precautions to ensure that the outsourced functions, services and bank client data can be brought back in-house or transferred to new cloud providers. These include in particular an appropriate termination period or the option to extend the existing operating model as well as a free choice of data export interfaces and formats.

7 See also FINMA Circ. 2018/3 "Outsourcing – banks, insurance companies and selected financial institutions under FinIA", margin no. 33 as well as Art. 9 para. 3 FADP.

B) Maintaining banking secrecy[8] in the cloud[9]

Purpose of the recommendations set out in the guidelines:
Compliance with the legal and regulatory requirements concerning **banking secrecy** should also be **ensured at all times in the cloud by means of appropriate technical and organisational measures.**

Whenever bank client data or personal data are being processed in the cloud, banking secrecy and data protection legislation need to be taken into account.[10]

The guidelines focus on processing data that are covered by banking secrecy, referred to here as bank client data. They discuss potential technical, contractual and organisational measures to appropriately limit the risk of bank client data being accessed by the cloud provider and its subcontractors (see Figure 2).

Definitions of terms[11]

Bank client data
Any information subject to the banking secrecy pursuant to Art. 47 of the Banking Act. Each institution determines for itself, within the framework of its business policy and the legal requirements, which specific information is to be classified as bank client data.

Personal data under the Federal Act on Data Protection (FADP)
Any information relating to an identified or identifiable natural person.[12]

8 These guidelines discuss banking secrecy by way of example, but the statements made apply analogously, for example, to professional confidentiality under Art. 69 of the Financial Institutions Act (FinIA). With reference to bank client data, trade secrecy under Art. 162 of the Swiss Criminal Code (SCC) and – where bank client data also qualify as personal data – the professional duty of confidentiality under Art. 62 FADP apply on a subsidiary basis.

9 See also chapter III:10 and chapter IV of the guidelines.

10 Where bank client data qualify as personal data, the provisions of the applicable data protection law also apply.

11 This is not an exhaustive list.

12 Art. 5 let. a FADP.

Foreign links and "foreign lawful access"[13]

Depending on an institution's operating model and the technologies employed, the cloud provider it uses may have foreign links. This may be the case, for example, if a cloud provider is owned by a foreign parent group or if it has its registered office or processes bank client data outside Switzerland.

When procuring cloud services, each institution must agree appropriate technical and organisational measures with its cloud provider in order to ensure that the cloud provider maintains the confidentiality of the bank client data and, for example, protects them against cyber criminals.

Where foreign links exist, however, there may be a residual risk that foreign authorities might have the power to demand disclosure of bank client data on the basis of applicable foreign laws. In such cases, the foreign authorities may process the bank client data on the basis of their applicable foreign laws, for example in the context of their own investigations or proceedings. Depending on the applicable foreign laws, a comparable level of protection and comparable rights (e.g. access and forwarding restrictions or legal recourse) to those in Switzerland may not be assured.

For reasons of practicability, it can be assumed in cases of doubt that foreign links may result in relevant foreign laws applying and may thus lead to access by foreign authorities that, while permitted under the applicable foreign laws, would not be permitted under Swiss law that apply to Swiss institutions (this is known as "foreign lawful access").

Where appropriate technical and organisational measures ensure with near certainty that either no data whatsoever are disclosed or that disclosure only concerns data that do not allow third parties who qualify as unauthorised under Swiss law to draw any conclusion, either directly or indirectly, concerning the identity of persons protected by banking secrecy, such disclosure is not relevant for the purposes of banking secrecy.[14] Alternatively, i.e. where appropriate technical and organisational measures cannot prevent either disclosure or identification with near certainty, it would be possible to obtain the consent of the persons concerned and, where necessary, authorisation from the competent authorities and thus justify disclosure to foreign authorities (see Figure 3).[15]

---

13 See also chapter III:10 margin no. 51 and chapter IV of the guidelines.

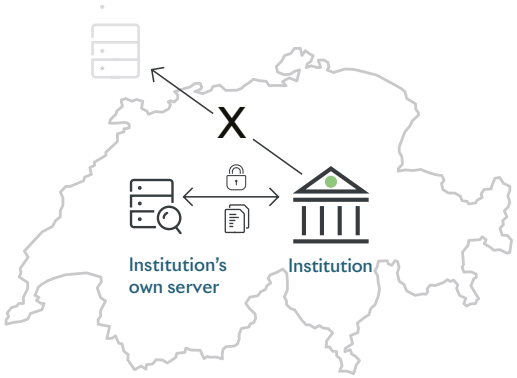
14 These data are also not qualified as personal data under data protection law in accordance with the relative method. This has been confirmed by the courts. See Federal Supreme Court ruling 136 II 508 – Logistep and the judgment of the Court of Justice of the European Union (CJEU) dated 19 October 2016 in case C-582/14 – Patrick Breyer versus the Federal Republic of Germany. See also recital 26 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) where applicable: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly."

15 See also chapter IV of the guidelines.

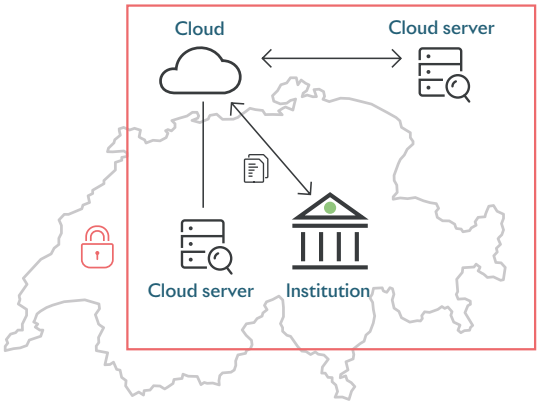
Figure 2

Banking secrecy in the cloud

Data currently protected on institution's own servers



Data protection in the cloud



Data protected in accordance with banking secrecy. In practice, jurisdiction marked the border in relation to control of data.

Data protected in accordance with banking secrecy by means of technical, organisational and contractual measures.

Source: Swiss Bankers Association (SBA) 2025

Protecting bank client data in the cloud[16]

Potential technical measures[17]

Appropriate technical measures may have the effect that the data processed in the cloud no longer constitute bank client data. Anonymised data therefore do not qualify as bank client data. The same may be true of pseudonymised or encrypted data from the perspective of the data recipient, for example if the recipient does not possess a concordance table for the pseudonyms or a means of decrypting the encrypted data.[18]

- **Anonymisation:** Anonymisation involves irreversibly changing personal attributes (e.g. a person's name or other identifiers) with near certainty so that no one can link it to the person concerned.
- **Pseudonymisation:** In pseudonymisation, personal attributes are replaced by an artificial identifier or pseudonym such that, while the institution can link them to the person concerned, it is almost certain that the recipient cannot.
- **Encryption:** Encryption is the main form of pseudonymisation. It involves using a key to convert cleartext[19] into an encoded text so that the original information can only be made readable again by using the correct key.

16 See also, for example, Annex C of the Federal Chancellery report of March 2025 on the legal framework for the use of public cloud services in the Federal Administration (2nd edition), which offers a general overview of the risks and mitigation measures.

17 See also chapter III:10.2 margin nos 38 et seqq. of the guidelines.

18 See also footnote 14.

19 Text in a readily understandable form, unencrypted information.

Potential organisational measures

- Appropriate monitoring by the institution of the operational measures implemented by the cloud provider and its subcontractors;
- Auditing of the cloud provider's security and confidentiality standards with reference to independent reports and on the basis of recognised reporting standards.

Potential contractual measures[20]

- Technical and organisational measures appropriately specified in the contract;
- Duty for the cloud provider to agree appropriate organisational and technical measures with its subcontractor;
- Agreement by the cloud provider to maintain confidentiality by means of specific requirements for technical and organisational measures;
- Consideration of the sensitivity of the data and imposition of a responsibility in this respect on the provider;
- Monitoring of the implementation of and compliance with the technical, organisational and contractual measures by the cloud provider and auditing by a recognised audit firm;
- Agreements on how the institution or cloud provider is to proceed in response to requests from the authorities or proceedings relating to the handover or transfer of bank client data that are processed in the cloud;
- Agreements on procedure on the part of the institution or cloud provider for identifying and assessing violations of confidentiality by cyber criminals and the like.

Interplay between legal requirements and TOM requirements and appropriate measures[21]

Both the legislator and the regulator often talk of a risk-based approach to requirements for technical and organisational measures (TOM requirements).[22] This does not mean that failing to comply with legal or regulatory requirements is a "calculated risk". In fact, the opposite is true.

20 Some institutions treat contractual measures as part of their organisational measures. However, technical and organisational measures are not normally to be regarded as legal matters or requirements.

21 See also chapter III:10.2 margin no. 37 of the guidelines.

22 See also e.g. the explanatory report on the Data Protection Ordinance (DPO) dated 31 August 2022, pp. 10, 17 et seq., 22, 28.

Compliance with the applicable legal and regulatory requirements must be assured in every case by means of independent technical and organisational measures.

The risk-based approach is used to define appropriate technical and organisational measures: depending on an institution's specific business and operating models as well as its strategies, the probability of and extent of losses resulting from a violation of the law may be higher in some scenarios than in others.

The risk-based approach means that the appropriate technical and organisational measures that are defined and correctly implemented do not have to address and prevent all theoretically conceivable scenarios. Instead, they must address and prevent the scenarios that, under normal circumstances and based on experience, are foreseeable and avoidable through due diligence. Should a scenario occur that was not foreseeable in this sense and could not be avoided despite the correct implementation of appropriate technical and organisational measures, this would not in principle constitute improper (illegal) conduct on the part of the institution or the decision-maker.[23]

Fully ruling out all risks is neither practicable nor required by law. The focus should be on exercising due diligence in every case by addressing the foreseeable institution-specific risks through the relevant roles, functions etc. along with appropriate technical and organisational measures.

C) Transparency and collaboration between institutions and cloud providers with regard to measures ordered by the authorities and the courts[24]

Purpose of the recommendations set out in the guidelines[25]:
A **coordinated procedure agreed by the cloud provider and institution** should be adopted in response to requests from foreign authorities involving the handover of bank client data.

23 See Federal Supreme Court ruling 135 IV 56, E.2.1. Various methods exist for assessing the probability of and extent of losses resulting from a violation of the law.

24 See also chapter IV of the guidelines.

25 The same recommendations may apply in particular to other forms of professional or business confidentiality, notwithstanding questions of data protection law that are not discussed here.

Requests from the authorities or proceedings may relate to the handover or transfer of bank client data that are processed in the cloud. Foreign laws can also provide for the handing over of data by cloud providers.

The guidelines recommend that the cloud provider and institution put in place a coordinated approach to dealing with requests from the authorities relating to the handover or transfer of bank client data.

Where a request for disclosure or transfer of bank client data from a competent Swiss authority (or a competent Swiss court) has an adequate and clear legal basis in Swiss law (including international treaties ratified by Switzerland), this is referred to as "lawful access". In this case, an assessment should be made as to whether the legal basis in question genuinely covers the specific disclosure or transfer.

A foreign authority citing a legal basis under its own national law, meanwhile, is termed "foreign lawful access". Disclosing bank client data may not be permitted under Swiss law (e.g. if the information concerned is protected by banking secrecy) – even if the foreign legal basis provides for the disclosure or transfer of bank client data. In such cases, as outlined above, previously implemented appropriate technical and organisational measures should be used either to prevent the disclosure of bank client data with near certainty or to ensure that disclosure only concerns information that does not allow third parties who qualify as unauthorised under Swiss law to draw any conclusion, either directly or indirectly, concerning the identity of persons protected by banking secrecy. Where this is not possible, an assessment should be made as to whether the specific disclosure or transfer to foreign authorities could be justified by the institution giving its consent[26], by the persons concerned giving their consent[27], by a decision from a competent Swiss court and/or by an authorisation from a competent Swiss authority (see Figure 3).[28]

Where the law permits, the cloud provider should always inform the institution in good time if approached by a foreign authority with a request to transfer or disclose bank client data in the cloud. Where the legal basis cited by the foreign authority forbids the cloud provider from informing the institution, the cloud provider should independently assess the legality of the request for disclosure and contest it if it does not comply with the legal requirements cited by the foreign authority.[29] When contesting a request, the cloud provider should take preventive measures to delay the effect of the request until the competent judicial authority has ruled on its legality. The cloud provider should only disclose the requested bank client data when required to do so under the applicable rules of procedure.[30]

It should also give the institution the rights to conduct the proceedings and support it in dealing with requests from foreign authorities.

---

26 Such consent may be provided and documented in various ways in line with the institution's risk management and risk tolerance with a view to securing evidence.

27 See footnote 26.

28 In connection with requests from foreign authorities and regardless of whether the information concerned qualifies as bank client data and/or personal data, further requirements such as Art. 42c of the Financial Market Supervision Act (FINMASA) and Art. 271 of the SCC are relevant; see the comments below in chapter IV of the guidelines.

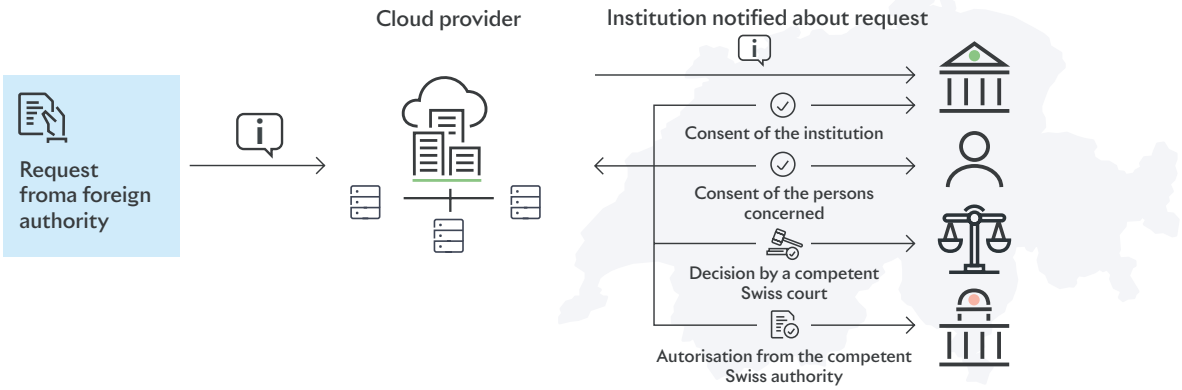
29 As set out in Clauses 15.1 "Notification" and 15.2 "Review of legality and data minimisation" of the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. s.

30 See footnote 29.

Figure 3

Requests from foreign authorities

Bank client data is handed over only under certain conditions



When the cloud provider receives a request from a foreign authority to hand over bank client data that is being processed in the cloud, the cloud provider must agree with the institution on how to proceed. If disclosure of bank client data cannot be prevented with near certainty by means of appropriate technical and organisational measures, bank client data may only be transferred in accordance with the applicable legal provisions and, depending on the individual case, with the consent of the bank, with the consent of the persons concerned, on the basis of a decision by a competent Swiss court and/or on the basis of an authorisation from the competent Swiss authority.

Source: Swiss Bankers Association (SBA) 2025

D) Audit of the cloud services and means used[31]

Purpose of the recommendations set out in the guidelines:

Third-party **access to data in the cloud for the purposes of auditing** should be guaranteed at all times.

Cloud services are normally delivered by providers from highly secure computer centres to a large number of clients. Auditing the infrastructures used requires a high degree of specialisation.

Cloud providers' compliance with the applicable legal, regulatory and contractual requirements should be audited at regular intervals. These include in particular requirements concerning outsourcing, data protection and information security. There should be provision for the audits to be carried out and ordered by the institution, its external auditors or FINMA. Pool audits by a number of institutions or their auditors as well as indirect or accompanied audits are permitted.

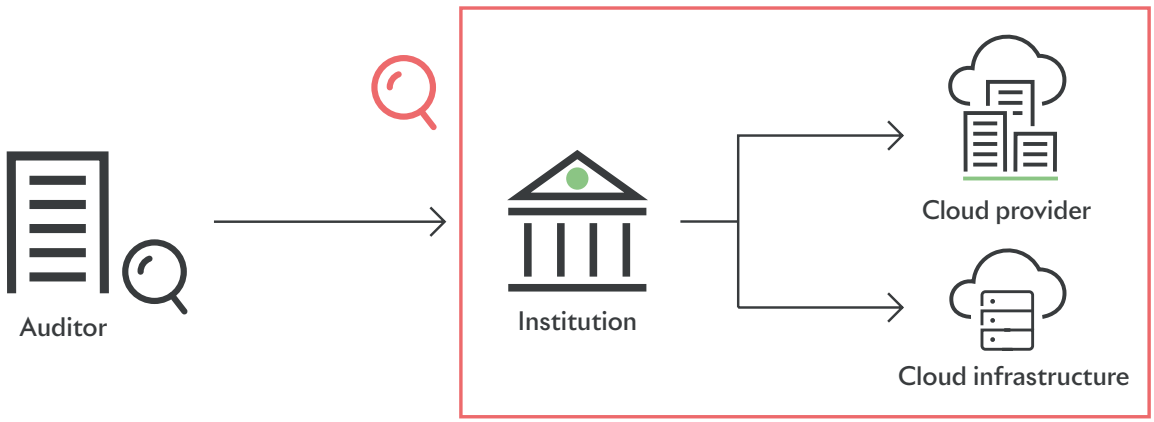
31 See also chapter V of the guidelines.

An on-site audit of the IT infrastructures actually used to deliver the cloud services is not absolutely necessary, except for inspecting the physical security measures. Logical access[32] will suffice. The institution's audit of the significant subcontractors can be carried out indirectly by auditing the cloud provider.

Figure 4

Auditing in the cloud

Auditing the cloud infrastructure requires a high degree of specialisation



The auditor should have at least logical access to the cloud infrastructure in order to audit the bank.

Source: Swiss Bankers Association (SBA) 2025

32 Technical access control or interaction with the hardware via remote access as opposed to physical access involving interactions with the hardware in the physical environment.

Legal and regulatory guidelines

for the

use of cloud services by banks and securities firms in the context of FINMA-regulated outsourcing

Contents

Chapter I: General provisions

1 Subject matter and purpose, scope of application, non-binding nature

(1)* These guidelines contain recommendations for institutions and providers on the procurement and deployment of cloud services. They are intended to be an aid to the interpretation of the legal and regulatory requirements in practice, with particular reference to the following four key areas:

- **Governance:** selection of the provider and its subcontractors, consent to a change of subcontractors (chapter II)
- **Data processing:** processing of bank client data[1] (chapter III)
- **Authorities and procedures:** transparency and collaboration between institutions and providers with regard to measures ordered by the authorities and the courts (chapter IV)
- **Audit:** auditing the cloud services and the cloud infrastructure used to deliver them (chapter V)

The experience now gained by various institutions has served to clarify the initial legal questions further, turning the cloud discussion away from legal issues and towards non-legal issues relating to the requirements for appropriate technical and organisational measures. These specify and operationalise the relevant business policy, legal and regulatory requirements, which are institution-specific and reflect the various business and operating models. When applying the guidelines, institutions may adopt a proportionate and risk-based approach for this purpose based on their size and the complexity of their business model.

(2) These guidelines have been developed with a view to cloud services that are delivered by providers to institutions and constitute outsourcing of significant functions as covered by FINMA Circ. 18/3.

(3)* These guidelines are non-binding and do not constitute self-regulation.

1 The guidelines focus on the processing of all data with relevance for banking secrecy. These are referred to here as "bank client data".

2 Terms

(4)* For the purposes of these guidelines, certain terms are defined as follows:

a. **"BA":** the Federal Act on Banks and Savings Banks (Banking Act, BA), SR 952.0.
b. **"banking secrecy":**[2] the secrecy protected under Art. 47 BA.
c. **"bank client data":** any information subject to the banking secrecy pursuant to Art. 47 of the Banking Act. Each institution subject determines for itself, within the framework of its business policy and the legal requirements, which specific information is to be classified as bank client data
d. **"BO":** the Ordinance on Banks and Savings Banks (Banking Ordinance, BO), SR 952.02.
e. **"clients":** the clients of an institution.
f. **"cloud" or "cloud computing":** as defined by the National Institute of Standards and Technology (NIST)[3] or the European Union Agency for Network and Information Security (ENISA)[4]; ocloud or cloud computing includes the Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) models, and can be supplied as public cloud, private cloud or hybrid cloud.[5]
g. **"cloud services":** the cloud computing service models supplied by the provider on order of the institution.
h. **"critical data":** data as defined in margin no. 7 of FINMA Circ. 23/1.
i. **"FADP":** the Federal Act on Data Protection, SR 235.1.
j. **"FinIA":** the Federal Act on Financial Institutions (Financial Institutions Act), SR 954.1.
k. **"FinIO":** the Ordinance on Financial Institutions (Financial Institutions Ordinance), SR 954.11.
l. **"FINMA Circ. 18/3":** Circular 2018/3 of the Swiss Financial Market Supervisory Authority, "Outsourcing – banks, insurance companies and selected financial institutions under FinIA", date of issue: 21 September 2017, in the currently valid version.
m. **"FINMA Circ. 23/1":** Circular 2023/1 of the Swiss Financial Market Supervisory Authority, "Operational risk and resilience – banks / Managing operational risks and ensuring operational resilience", date of issue: 7 December 2022, in the currently valid version.
n. **"FINMASA":** the Federal Act on the Swiss Financial Market Supervisory Authority (Financial Market Supervision Act), SR 956.1.
o. **"guidelines":** the principles and recommendations set out in this document.
p. **"institution":** banks and securities firms as defined in margin no. 5 of FINMA Circ.18/3.
q. **"ISA":** the Federal Act on Information Security in the Confederation (Information Security Act), SR 128.

---

2 These guidelines discuss banking secrecy by way of example, but the statements made may be applicable analogously, for example, to professional confidentiality under Art. 69 FinIA. With reference to bank client data, trade secrecy under Art. 162 SCC and – where bank client data also qualify as personal data – the professional duty of confidentiality under Art. 62 FADP apply on a subsidiary basis.

3 The NIST Definition of Cloud Computing (2011)

4 European Network and Information Security Agency (ENISA), Cloud Computing Security Risk Assessment (2009)

5 "Cloud" and "cloud computing" also include, for example, "function as a service" (FaaS).

r. **"personal data":** as defined in the data protection legislation. The term "personal data" also includes the term "personal information ."[6]
s. **"processing":** as defined in the Federal Act on Data Protection.[7]
t. **"provider":** the provider of the cloud services outside the institution or the institution's company group.
u. **"reporting obligation":** the duty to notify under Art. 24 FADP, Art. 74a et seqq. ISA, FINMA Guidance 05/2020 "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA"[8] and FINMA Circ. 23/1, margin no. 81.
v. **"SCC":** the Swiss Criminal Code, SR 311.0
w. **"significant subcontractors":** subcontractors that, as part of the delivery of cloud services by the provider, (i) perform significant functions within the meaning of FINMA Circ. 18/3 or (ii) in the institution's view are to be regarded as significant subcontractors.

6 As defined in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) where applicable.

7 As defined in the General Data Protection Regulation where applicable.

8 FINMA specifies the requirements for reporting cyber attacks in its Guidance 03/2024 of 7 June 2024.

Chapter II: Governance (including risk management)

Legal basis

- Arts 3 and 47 BA, Art. 12 BO
- Arts. 2, 5, 6, 9, 41 et seqq. and 69 FinIA and Arts. 66 and 68 FinIO
- FADP
- FINMA Circ. 23/1
- FINMA Circ. 18/3

3 Decision to procure cloud services

(5) Cloud computing covers a wide variety of available services, ranging from highly standardised cloud infrastructures and services to bespoke solutions. The decision to procure cloud services should therefore be taken on the basis of a structured process.

(6)* If the decision to procure cloud services is taken on the basis of a risk analysis[9] carried out in advance, this should take account not just of the opportunities and risks associated with using cloud services but also of the significance of the cloud services for the purposes of FINMA Circ. 18/3 and the categorisation of the data, in particular bank client data, processed as part of the cloud services.

(7) When assessing the risks, the institution should also take into account those that may be associated with the inadequate delivery of the cloud services or the total or partial failure of those services or of the provider.

(8)* If there are risks associated with the procurement, deployment or termination of the use of the cloud services, appropriate mitigating measures should be defined and implemented, further developed and monitored as part of risk management for as long as the cloud services are being used. As a result, following the procurement phase ("change the bank"), an adequate structure and process organisation should be created to ensure smooth operation ("run the bank") of cloud services by means of appropriate technical and organisational measures, documentation[10], controls and governance.

---

9 For example, this would include assessing the risks associated with data security or operational risks.

10 In particular in the case of service contracts containing links to appendices, the institution should download and store the appendices valid at the time the contract is signed.

4 Responsibilities and roles

(9)* In view of the regulation the institution is subject to, account must be taken of financial market legislation as well as – where bank client data or personal data are processed as part of the cloud services – banking secrecy and the data protection act.[11]

(10) When allocating responsibilities and defining roles, the service and delivery models must be considered. The provider should cooperate as appropriate and necessary, making relevant information available to the institution. Ideally this cooperation should begin during the tender process.

(11) If the provider uses subcontractors to deliver the cloud services, due account should be taken of this when defining the roles and responsibilities with regard to the significant subcontractors.

(12) The contract between the institution and the provider should set out the corresponding rights and duties of the parties and others involved, and should also cover their implementation.

5 Selecting and changing the provider and significant subcontractors

(13) Providers (especially providers of highly standardised cloud services) routinely reserve the right to define and change the operating models, the technologies used, service providers within and outside the group, and other essential factors (design authority), with a view to efficient and competitive service delivery.

(14)* When selecting the appropriate provider it is in the institution's interest to take account of the provider's ability to fulfil the specific needs regarding technical and organisational measures as well as the contractual obligations, its financial stability and the jurisdictions to which it and its subcontractors are subject, as well as other essential points.[12] Significant subcontractors should be included in the assessment. The provider should assist as appropriate in gathering the information on this matter requested by the institution.

(15) The risk assessment should in particular include defining the mitigating measures and the responsibilities for implementing them.

(16)* When selecting a provider, its willingness to assume responsibility for the essential duties arising out of financial market[13] and data protection legislation and the design of its operating model should be considered in addition to performance-related criteria. When selecting a provider and its subcontractors to process bank client data from the institution or other personal data, the

---

11 Federal Act on Data Protection including its Ordinance and the General Data Protection Regulation where applicable.

12 Where personal data are processed, the checking duties set out in the FADP, e.g. in connection with data protection impact assessments and order processing, must be observed, with the content and scope of such checks tailored to the specific institution and its business and operating model.

13 Including appropriate confidentiality provisions.

security (i.e. confidentiality, integrity, availability and traceability) of the data must be a decisive criterion and an integral part of the underlying due diligence.[14]

(17)* A change of provider (e.g. a group company in another jurisdiction) should be subject to the prior consent of the institution, which may be given in writing or another verifiable manner. A restructuring that is purely internal to the group and within the same jurisdiction that does not have a material impact on the existing circumstances, criteria and risks may be exempted from this consent requirement. The provider should, at the institution's request, agree to put in place arrangements governing a change of the company controlling the provider or a significant subcontractor.

(18)* The involvement of new significant subcontractors or a change of subcontractors must be conducted in accordance with the principles set out in FINMA Circ. 03/18.[15] A contractual agreement on criteria for the involvement of significant subcontractors, with the provider required to ensure compliance and demonstrate fulfilment to the institution in advance, can give the institution additional security. In any event the institution must be notified before the provider involves a new significant subcontractor and given the opportunity to terminate the provision of services by the provider by a specific deadline, for good or justified reason where appropriate. In such cases the institution should take suitable precautions – in particular allowing itself an appropriate termination period and requiring appropriate cooperation on termination from the provider, as well as, if necessary, options to extend while maintaining the existing operating model as well as the free choice of data export interfaces and formats – so that the outsourced functions and services and bank client data can be returned or transferred to a new provider. Lock-in effects and the amount, number and criticality of the outsourced functions and bank client data should be taken into account.

6 Data centres and operating centres

(19)* Concerns are sometimes expressed that the use of cloud services means that it is no longer possible to identify where the data are being processed (data ubiquity). From the institutions' perspective, their clients' trust in the way their data are handled is of central concern.

(20) The provider should disclose the locations where the cloud infrastructures (data centres) that the institution deploys (or can deploy) are situated and from which the cloud is operated (operating centres), as well as changes of location during the period of deployment. This disclosure should include information on the (legal) entities, specifically the provider and significant subcontractors, that operate, own or otherwise control the data centres and operating centres.

---

14 Clear criteria governing the assessment of how the provider handles critical data must be defined and verified before the contract is signed (see FINMA Circ. 23/1, margin no. 82).

15 FINMA Circ. 03/18, margin no. 33.

(21)* A change of location to another jurisdiction during the term of the contract should be subject to a contractually defined change procedure and, depending on the individual need for protection, require the prior consent of the institution, at least where personal data are processed or the subcontractors qualify as significant.[16] The provider should detail the risks associated with the change of location and supply the institution with all the relevant information, in particular regarding the security measures applied, to enable it to take a decision.

(22)* Further requirements arising out of data access by third parties are described in the following chapters.

Chapter III: Data and data security

Legal basis

- Art. 47 BA
- Art. 69 FinIA
- FINMA Circ. 23/1
- FINMA Circ. 18/3
- FADP

7 Classification of data and information

(23)* To enable proper implementation of the requirements under data protection legislation and ensure that banking secrecy is maintained, the requirements of FINMA Circ. 23/1 regarding critical data should also be observed. Accordingly, the institution should identify and classify the bank client data processed by means of the cloud services.

(24)* This should allow the institution, and where relevant the provider, to assess and define the applicable legal and regulatory requirements with regard to data processing and data flows, access concepts and the appropriateness of further technical and organisational measures, including controls.

16 With regard to consent, extension options and possible termination of the contract, the principles set out in margin no. 18 apply.

(25)* Consideration should be given to whether, and to what extent, clients have been informed that processing of bank client data has been outsourced to a provider of cloud services in Switzerland or abroad or, if and to the extent necessary, they have agreed to such outsourcing.[17]

(26)* Material changes to the classification of the outsourced bank client data during the term of the contract should be recorded and necessary measures taken before such outsourcing.

8 Storage locations and data flows, access concept

(27)* The provider should allow the institution to review[18] the locations where the bank client data are processed (and in particular stored) and control those locations by means of technical and organisational measures. The institution should also be in a position to comply with its duties of transparency to clients and therefore know where processing is carried out (in particular the locations where bank client data are stored) to the level of detail required for this purpose.

(28)* Data flows involving bank client data, which take place in the sphere of the provider and, where relevant, its subcontractors, should be disclosed to the institution in advance and the architecture underlying the data flows should, where required, be specified as precisely as necessary by means of technical and organisational measures and stipulated in the contract.

(29)* The latter also includes the definition and implementation of an access concept[19] by the provider. The provider should disclose access authorisations granted on request, and access to bank client data should be monitored and recorded in an appropriate manner by the provider.

(30)* The access concept should also define the purpose of access in sufficiently narrow terms and indicate the precisely defined cases in which access to systems used to process bank client data can be granted or is unblocked. Such cases may include emergencies or other critical failures of the cloud infrastructure that cannot be remedied in any other way.

9 General technical and organisational measures on data security

(31)* In general, the provider should offer and, in accordance with the agreement, implement appropriate technical and organisational measures to protect the institution's bank client data that it is processing and stipulate these in the contract. International and local technical standards[20] should be taken into account. The provider should also agree appropriate technical and organisational measures with its subcontractors.

---

17 See Chapter III:10 below.

18 The requirements for such an audit are set out in Chapter V below.

19 With regard to access to bank client data.

20 E.g. standards set by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) (professional standards).

(32)* The provider should ensure that its staff and those of the subcontractors that have access to bank client data verifiably undertake to maintain confidentiality and treat the data accordingly, receive information and training to this effect, and are monitored using suitable measures.[21] This undertaking by the staff is deemed to be sufficient if it is made to the provider or its subcontractors as part of the employment relationship. It is recommended that providers comply with data protection law and expressly advise their staff working in Switzerland of banking secrecy and other applicable legal confidentiality obligations, as well as of the fact that breaching it is a criminal offence.

10 Banking secrecy and security measures

10.1 Introductory remarks

(33)* Before deploying cloud services, the institution must clarify whether it is necessary to obtain a waiver of banking secrecy (Art. 47 BA)[22] from the client. This would be the case in particular if the institution were to conclude that it could not prevent the disclosure of bank client data to unauthorised persons with near certainty by means of appropriate technical and organisational measures and would thus risk intentionally or negligently breaching banking secrecy.

(34)* This document argues that a waiver of banking secrecy by the client is not necessary, provided the institution has put in place adequate technical, organisational and contractual security measures covering the bank client data processed using the cloud services in order to exclude out the disclosure of bank client data to unauthorised persons with near certainty.

This chapter contains an overview of the arguments supporting this interpretation and the security measures to be taken.

10.2 Potential technical, organisational and contractual measures[23]

(35)* An actual **disclosure** of bank client data to unauthorised persons caused intentionally or negligently by the institution constitutes a breach of banking secrecy.[24] Art. 47 para. 1 BA is a result crime: the mere possibility that unauthorised persons may obtain knowledge of bank client data does not in itself constitute a breach of banking secrecy.

(36)* Therefore, if the provider and its subcontractors do not actually obtain knowledge of the bank client data being processed in the cloud as part of the cloud services, there is no disclosure within the meaning of Art. 47 para. 1 BA. However, the institution must have put in place appropriate

21 See FINMA Circ. 23/1, margin no. 80.

22 See footnote 2.

23 Some institutions treat contractual measures as part of their organisational measures. However, technical and organisational measures are not normally to be regarded as legal matters or requirements.

24 See judgment of the Federal Supreme Court 6B_1403/2017 of 8 August 2017.

technical, organisational and contractual measures to limit the risk of the provider and its subcontractors accessing the bank client data.

(37)* The measures to be implemented are set out in the applicable legal and regulatory provisions.[25] However, assessing the appropriateness of these measures is not a legal matter and should take account of the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of processing the bank client data, as well as the differing probabilities of occurrence and gravity of the risk for the rights of the clients affected.

It can be borne in mind here that, depending on an institution's specific business and operating models as well as its strategies, the probability of and extent of losses resulting from a violation of the law may be higher in some scenarios than in others. Appropriate technical and organisational measures therefore do not have to address and prevent all theoretically conceivable scenarios. Instead, they must address and prevent the scenarios that, under normal circumstances and based on experience, are foreseeable and avoidable with near certainty through due diligence.[26] Dabei muss die im Einzelfall erforderliche Sorgfalt eingehalten werden.

Some examples of measures are listed below.[27]

(38)* **Appropriate technical measures to protect bank client data:**

Appropriate technical measures may have the effect that the institution no longer has to classify the data processed in the cloud as bank client data. Anonymised data therefore do not qualify as bank client data. Accordingly, anonymized data does not qualify as bank client data. The same may be true of pseudonymised or encrypted data from the perspective of the data recipient, for example if the recipient does not possess a concordance table for the pseudonyms or a means of decrypting the encrypted data.[28]

The following security measures are particularly suitable technical processes for appropriately protecting bank client data.

(39)* Anonymisation: Data anonymised with near certainty (irreversible method) no longer constitute bank client data and/or personal data. The requirements set out in this section therefore do not apply to anonymised data.

---

25 See also FINMA Circ. 23/1, margin no. 79.

26 See Federal Supreme Court ruling 135 IV 56, E. 2.1. This is also known as the risk-based approach. Various methods exist for assessing the probability of and extent of losses resulting from a violation of the law.

27 See also, for example, Annex C of the Federal Chancellery report of March 2025 on the legal framework for the use of public cloud services in the Federal Administration (2nd edition), which offers a general overview of the risks and mitigation measures.

28 These data are also not qualified as personal data under data protection law in accordance with the relative method. This has been confirmed by the courts. See Federal Supreme Court ruling 136 II 508 – Logistep and the judgment of the Court of Justice of the European Union (CJEU) dated 19 October 2016 in case C-582/14 – Patrick Breyer versus the Federal Republic of Germany. See also recital 26 of the General Data Protection Regulation where applicable: *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly."*

(40)* Pseudonymisation: Where the data constitute bank client data, the assignment rule should be appropriately protected under the institution's control. In particular, the rights to use the reference table should be restricted on a need-to-know basis and access documented in a verifiable manner.

(41)* Encryption: When encrypting bank client data, care should be taken to ensure that the encryption key is protected against unauthorised access and access remains under the institution's control, even if the encryption key is also available to the provider or kept by it and used for the automated encryption and decryption of the bank client data as part of the cloud service. With regard to the classification of bank client data in particular, the institution should, on the basis of a risk assessment, consider which procedures are appropriate to define the control of the encryption key.

The encryption procedure and the strength of the encryption key must meet current security standards, so that the encryption can be regarded as cryptographically secure. This is determined by the state of the art (rules of professional practice).

Bank client data should in principle be transferred in encrypted form. The encryption procedure and the strength of the encryption key must meet current security standards, so that the transfer can be regarded as cryptographically secure.

(42)* **Organisational measures to protect bank client data:**

The operational measures implemented by the provider and its subcontractors should be subject to appropriate supervision by the institution.

The required audit of the provider's security and confidentiality standards should be conducted with reference to independent reports and on the basis of recognised reporting standards.[29]

(43)* **Contractual measures to protect bank client data:**

Contractual measures generally reflect the agreed technical and organisational measures and include in particular:

- appropriate stipulations in the contract between the provider and the institution regarding the technical and organisational measures and a requirement for the provider to agree appropriate organisational and technical measures with its subcontractors;
- an agreement by the provider to maintain confidentiality by means of specific requirements for technical and operational measures;
- taking account of the sensitivity of the data and imposing a responsibility in this respect on the provider;
- monitoring the implementation of and compliance with the technical, organisational and contractual measures;

29 For example, the auditing standards of the reporting options under ISAE 3000 or SOC2.

- agreements as per chapter IV (Authorities and proceedings) and on the procedure for identifying and assessing violations of confidentiality by cyber criminals and the like.[30]

10.3 Persons subject to the duty of confidentiality

(44)* Depending on the cloud service model, it may be necessary for staff of the provider and its subcontractors to process the bank client data in the cloud in cleartext, i.e. neither encrypted respecitvely pseudonymised, and therefore actually obtain knowledge of them. In this event, the question arises as to whether the provider and its subcontractors constitute unauthorised persons for the purposes of Art. 47 para. 1 BA. For the sake of clarity, fully automated encryption and decryption as part of the cloud service is not to be viewed as cleartext data processing for the purposes of this section.

(45) The provider and its subcontractors do not constitute unauthorised persons within the meaning of Art. 47 para. 1 BA. The deployment of cloud services of a provider in principle reflects the institution's sincere interest in optimising service quality, costs and data security. The dispatch on the revision of the BA explicitly refers to the status of IT service providers as representatives (representative in the meaning of Art. 47 para. 1 BA; "Beauftragte").[31] Additionally, the institution normally has the right to issue instructions[32] to the provider and its subcontractors. They are therefore to be regarded as representatives for the purposes of Art. 47 para. 1 BA and can be categorised as persons subject to the duty of confidentiality.

(46)* Providers and subcontractors based outside Switzerland are also representatives and, as such, authorized persons subject to the duty of confidentiality. This corresponds to the meaning and purpose of Art. 47 para. 1 BA and is not excluded by the wording.[33]

(47) However, the increased risk resulting from processing of data in cleartext outside Switzerland must be taken into account as part of the applicable security measures. The key criteria for assessing appropriateness may include country-specific risks, in particular (but not limited to) the issue of whether the respective legislation ensures adequate data protection.

(48)* The relevant technical, organisational and contractual measures are also set out in the applicable legal and regulatory provisions.[34]

---

30 In this case, depending on the data concerned (object of protection), various legal basis may apply, entailing various clarifications, deadlines and reporting thresholds and various authorities being in charge of; see e.g. Art. 24 FADP, FINMA Guidance 05/2020 "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA", FINMA Circ. 23/1 margin no. 81 and Art. 74a et seqq. ISA . With regard to the contract with the provider ist has to be taken into account that these reporting obligations do not exclusively concern bank client data.

31 Dispatch on the revision of the BA dated 13 May 1970, BBL 1970, 1182: *"The extension [of the duty of banking secrecy] to representatives is also to include in particular computer centres entrusted by banks with electronic data processing."*

32 FINMA Circ. 03/18, margin no. 21.

33 The need for an explicit exclusion follows from the legality principle of Art. 1 of the Swiss Criminal Code.

34 See also FINMA Circ. 23/1, margin no. 79.

(49) The additional technical and organisational measures listed below can be regarded as appropriate in relation to an increased risk outside Switzerland.

- Processing of data in cleartext by staff of the provider or its subcontractors outside Switzerland should only take place to the extent necessary for the secure and reliable operation of the cloud, and subject to narrowly defined conditions with respect to time and subject matter.
- Processing activities must be monitored and recorded by the provider and the institution should have the option to retain control over the timing, duration and scope of processing. The provider must be in a position to terminate processing without delay where there is a suspicion of unauthorised processing activity.
- The institution must be informed about the processing by the provider or must have the opportunity to obtain information itself.
- The institution must attach particular importance to the agreements under chapter IV (Authorities and proceedings).

(50)* As indicated above, cleartext processing of bank client data by staff of the provider and its subcontractors does not in principle constitute disclosure to unauthorised persons and thus does not represent a breach of banking secrecy by the institution.

(51)* Bank client data could be assumed to have been disclosed to unauthorised persons if third parties outside the sphere of the provider, such as foreign authorities, obtain knowledge of bank client data due to the use of cloud services. Foreign links may result in relevant foreign laws applying and may thus lead to access by foreign authorities that, while permitted under the applicable foreign laws, would not be permitted under Swiss law that applies to Swiss institutions (this is known as "foreign lawful access"). Where previously implemented appropriate technical and organisational measures either prevent the disclosure of bank client data with near certainty or ensure that disclosure only concerns information that does not allow third parties who qualify as unauthorised under Swiss law to draw any conclusion, either directly or indirectly, concerning the identity of persons protected by banking secrecy, no deliberate or negligent act (and thus no criminal violation of banking secrecy) has been committed.[35]

10.4 The institution's duties to inform

(52)* Any duty under data protection legislation for persons concerned to be informed that their personal data are being processed by the provider and its subcontractors is governed solely by that legislation. Consequently, such information may be provided in general form via the institution's general data protection policy without details being given as to each specific processing by the provider and its subcontractors.

35 This means that, in a case where there is a mere possibility of accessing bank client data, the assumption of a criminal attempt at disclosure to unauthorised parties does not arise.

(53) Further duties to inform that may arise for reasons other than data protection law must be assessed on a case-by-case basis. Attention must be paid, for example, to the expectation horizon of the client as well as contractual agreements, provisions under contract law and the principle of good faith. Reference could be made e.g. to the institution's market presence and communication with regard to its past use of service providers.

11 Measures to secure the availability and return of information

(54)* The institution should be able to access any bank client data that are stored or processed abroad or in Switzerland at any time from Switzerland. The provider should undertake to continue to deliver the cloud services to the institution, a successor company or rescue company and, where applicable, FINMA if the institution is in recovery or resolution, to the extent that such access from Switzerland to information abroad or in Switzerland is assured as a result.[36]

(55)* The provider should undertake to return the bank client data to the institution, a successor company or rescue company at any time as part of assistance with termination, if the institution is in recovery or resolution and on the instructions of the institution or FINMA, provided the provider has the means[37] and knowledge[38] to do so. In this case, the provider should transfer the bank client data back in a standardised, machine-readable format chosen by the institution.

(56) If the provider uses proprietary solutions that result in lock-in effects, the provider should declare its willingness to support the institution with a migration to other solutions or with licensing such solutions.[39]

---

36 For significant outsourcing, see FINMA Circ. 18/3, margin no. 31.

37 Such as encryption keys.

38 Especially where cloud services as part of IaaS or PaaS are concerned, the provider may have no knowledge of the architecture chosen by the institution and/or the components used by the institution.

39 Depending on the scope of application, foreign legal basis in particular, e.g. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) may impose additional legal requirements in relation to these aspects.

Chapter IV: Authorities and Proceedings

Legal basis

- Art. 271 SCC
- Art. 273 SCC
- Art. 47 BA
- Art. 6 et seq. FADP
- International treaties on international legal assistance
- FINMA Circ. 23/1
- Art. 42c FINMASA

(57)* The provider must agree with the institution a procedure for both parties to adopt in response to requests from the authorities relating to the handover or transfer of bank client data that are processed in the cloud.[40] To the extent that there is no conflict with mandatory law, the provider must supply the institution with a contractual undertaking covering the technical and organisational measures set out in margin nos 58–60.

(58)* In the context of foreign proceedings the provider, its subcontractors and group companies may only transfer or disclose bank client data processed in the cloud to foreign authorities or other parties abroad in accordance with the applicable legal and regulatory provisions and, depending on the individual case, (i) with the prior consent of the institution[41], (ii) with the prior consent of the persons concerned[42], (iii) on the basis of a decision by a competent Swiss court (iv) and/or on the basis of an authorisation from the competent Swiss authority.

(59)* The provider should notify the institution in due time prior to handing over the bank client data, give the institution the rights to conduct the proceedings, and support the institution in handling requests from foreign authorities.

(60)* If, on account of mandatory law, the provider is unable to notify the institution in advance of the transfer or disclosure of bank client data to foreign authorities or other parties abroad, the

40 The same principles may apply in particular to other forms of professional or business confidentiality, notwithstanding questions of data protection law that are not discussed here.

41 Such consent may be provided and documented in various ways in line with the institution's risk management and risk tolerance with a view to securing evidence.

42 See footnote 41.

provider should implement the appropriate legal or protective measures within the scope of the agreement made and in the interest of the institution and its clients.[43] The provider should also independently assess the legality of the request for disclosure and contest it if it does not comply with the legal requirements cited by the foreign authority. When contesting a request, the provider should take preventive measures to delay the effect of the request until the competent judicial authority has ruled on its legality. The provider should only disclose the requested bank client data when required to do so under the applicable rules of procedure.[44]

(61)* In addition, the provider should inform the institution in a general way of the number (per year), subject matter and conduct of proceedings that involve or could involve the transfer or disclosure of bank client data under applicable foreign law or regulations and that are applicable to the provider and the subcontractors[45] or group companies of the provider.[46]

(62) The institution should, with appropriate cooperation from the provider where necessary, assess the risks of foreign authorities being able to override the effectiveness of the technical, organisational and contractual measures in accordance with margin no. 10.[47]

43 See chapters II and III, in particular the comments on bank-client confidentiality and transparency under data protection law.

44 As set out in Clauses 15.1 "Notification" and 15.2 "Review of legality and data minimisation" of the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

45 Subcontractors that have access to bank client data.

46 See footnote 37.

47 See margin no. 37.

Chapter V: Audit of the cloud services and means used

Legal basis

- Arts 18 and 23 et seqq. BA and the implementing provisions of the BO
- Arts. 61 and 63 FinIA
- FINMA Circ. 23/1 margin nos. 71-82 as well as related audit points on the management of risks involving critical data
- FINMA Circ. 18/3

(63) Cloud services are normally delivered by providers from highly secure computer centres to a large number of customers.[48] Auditing the infrastructures used by the providers requires a high degree of specialisation; account should be taken of the provider's duties of confidentiality to its other customers.

(64) Compliance with the requirements contractually imposed on the provider (including technical and organisational measures) arising out of the legal and regulatory requirements (in particular with regard to outsourcing, data protection and information security) should be audited regularly, taking account of the fact that the effectiveness of measures results from a combination of controls at the provider and at the institution. The provider should assist in this process to an appropriate extent. Performance of the contractually agreed services may also form part of the audit.

(65) There should be provision for the audits to be carried out and ordered by the institution, its external auditors or FINMA.[49] Pool audits by a number of institutions or their audit firms, as well as indirect or accompanied audits in which auditing and reporting are conducted by the provider's audit firm or an audit firm designated by the provider are permitted, provided the audit firm has the necessary independence and specialist expertise. This also applies to audits ordered by FINMA.

(66) An on-site audit of the IT infrastructures actually used to deliver the cloud services is not absolutely necessary, except for inspecting the physical security measures. Granting the institution, its audit firm or the competent authority logical access can be regarded as sufficient. The provider can agree the arrangements for this right of access directly with the supervisory authority.

48 Public cloud.

49 For significant outsourcing, see FINMA Circ. 18/3, margin no. 26.

(67) In the case of cloud services with links outside Switzerland, a contractual agreement covering the right for the institution, its audit firm, the provider's audit firm and FINMA to audit the provider directly or indirectly satisfies the requirement for appropriate clarification of audit rights.

(68) The principles set out above should also be prescribed in relation to significant subcontractors. In the absence of an agreement between the institution and the subcontractors, this should be done by binding the subcontractors to comply with the provider's contractual obligations.

(69)* The audit of the significant subcontractors can be carried out indirectly by auditing the provider, though a direct audit of the significant subcontractors may become necessary and must therefore be contractually agreed with the provider.

The legal and regulatory guidelines have been amended with effect from November 2025 as follows:

Amended margin numbers	1, 3, 4, 6, 8, 9, 14, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 48, 50, 51, 52, 54, 55, 57, 58, 59, 60, 61 and 69
Amended legal basis (box) in	chapters II, III, IV, V
Adapted terminology in	margin numbers 1, 4, 6, 9, 16, 18, 23, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 50, 51, 54, 55, 57, 58, 59, 60 and 61 as well as in footnotes 19, 35 and 45
Amended footnotes	9, 13, 15, 19, 35, 45 and 46
Newly added footnotes	1, 2, 3, 6, 7, 8, 10, 11, 12, 14, 16, 18, 20, 21, 22, 23, 25, 26, 27, 28, 30, 34, 36, 39, 40, 41, 42, 44, 47 and 49
Other	Deletion of the title of Chapter III:10.5 (before margin number 53); adjustment of the title of chapter II, chapter III:10.2 and III:10.4

Swiss Bankers Association
Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel
office@sba.ch
www.swissbanking.ch