LAUX LAWYERS AG
ZURICH | BASEL

ZURICH OFFICE
A Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BASEL OFFICE
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

ATTORNEYS-AT-LAW
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

Each registered with the
competent attorneys' register

Legal Opinion

Use of Cloud Offerings by Banks: Admissibility under Art. 47 Banking Act

Also, a contribution to the discussion on the occasion of the publication of a cloud guide by the Swiss Bankers Association (SBA) on the use of Cloud Offerings by banks and securities dealers.

(Convenience Translation of German Original)

Authors:
Dr. Christian Laux
Alexander Hofmann
Mark Schieweck
Dr. Jürg Hess

Zurich, February 14, 2019

MANAGEMENT SUMMARY

Purpose: The present Legal Opinion discusses the extent to which and the conditions under which a Bank[1] may use Cloud Offerings[2]. The analysis is limited to the criminal law aspects of Swiss Banking Secrecy and is based on three specific questions:

- Question 1: (a) Can a Swiss Bank use Cloud Offerings in light of Art. 47 of the Federal Law on Banks and Savings Banks (Banking Act)? (b) Is the answer different for foreign Cloud Offerings[3]?
- Question 2: (a) Can a Cloud Provider[4] act as an "Agent" within the meaning of Art. 47 Banking Act, and is the disclosure of bank customer data to the Cloud Provider punishable under Art. 47 Banking Act in such cases? (b) Is the answer different for foreign Cloud Offerings?
- Question 3: According to Art. 47 Banking Act, is it permissible for a Cloud Provider not appointed as an Agent to access secret information, as long as this is purely for operational purposes (especially IT maintenance or support)?

The result: According to our opinion, mature domestic and foreign Cloud Solutions are open to Banks for use. The Bank as a user must carefully select the Cloud Provider and take effective measures to ensure that the data it wishes to migrate is still protected in the IT Infrastructures[5] of the Cloud Provider. The aim of these measures is to avoid criminally relevant disclosures during Normal Operation[6]. To ensure this on a permanent basis, the Bank needs to understand how its perimeter, as extended by the Cloud Solution, is protected. This response is as follows:

Question 1: If the Bank selects Cloud Providers who can ensure – in technical, organizational and contractual terms – that, during Normal Operation, no disclosure to unauthorized outsiders occurs, the Bank may use their Cloud Offerings. Experience shows that this is already the case today for mature Cloud Providers. The migration of data to the IT Infrastructures of such Cloud Providers does not meet the conditions for a “disclosure”. Therefore, there is no criminally relevant event, irrespective of what the answer to questions 2 and 3 may be (sub-question 1a). The question of an international perspective is irrelevant for such Cloud Offerings (sub-question 1b).

Question 2: A Cloud Provider can be established as an Agent within the meaning of Art. 47 para. 1 lit. a Banking Act. The personal perimeter of the Bank is thereby extended. The Bank must ensure that the Cloud Provider has implemented protective measures of a technical, organizational and contractual nature. The migration of data to the IT Infrastructure of the Cloud Provider is not a disclosure (**privilege effect** for the benefit of Bank's Agents in criminal matters). This means there is no criminal liability on the part of the Bank (or of its officers and employees) even if the Cloud Provider has Plaintext Access[7] to protected information. The privilege is not provided automatically simply because someone performs a service for the Bank. In other words, Cloud Providers do not automatically become Agents. Therefore, it is important to note that a Cloud Provider can oppose being involved in the Bank's sphere of risk (and

---

1 For the term “Bank” see also the definition of the term in the Appendix.
2 For the term “Cloud Offering” see also the definition of the term in the Appendix.
3 For the terms “Foreign Cloud Offering / Provider” see also the definition of the term in the Appendix.
4 For the term “Cloud Provider” see also the definition of the term in the Appendix.
5 For the term “IT Infrastructure” see also the definition of the term in the Appendix.
6 For the term “Normal Operation” see also the definition of the term in the Appendix.
7 For the term “Plaintext Access” see also the definition of the term in the Appendix.

being established as an Agent). However, if the Cloud Solution has a good maturity level (as provided under question 1), then the Bank can still take advantage of it.

The privilege can also be affirmed for data to be migrated to IT Infrastructures of a foreign Cloud Provider. The decisive factor for this conclusion is the wording of the provision in Art. 47 para. 1 lit. a Banking Act. The use of foreign Agents is not excluded. Art. 1 of the Swiss Criminal Code ("no punishment without law") excludes different treatment of foreign Cloud Offers. This conclusion must be clarified by a supplementary interpretation of the criminal law aspect in Art. 47 Banking Act. The interpretation leads to the conclusion that involving foreign Agents does not lead to criminal liability.

The privilege allows the Bank to use a Cloud Provider, even if Plaintext-Access to protected information may take place by the Cloud Provider (or its employees or sub-contractors) in a controlled manner during Normal Operation (sub-question 2a). This also applies to foreign Cloud Providers (sub-question 2b).

Question 3: There is little room left for question 3 after answering questions 1 and 2. To the extent to which the Cloud Provider has been appointed as an Agent, the problem does not arise per se (privileged information exchange without criminal liability). Also, for many of the operational measures to be discussed under question 3, it will be possible to confirm for mature Cloud Providers that no disclosures will take place (then the analysis for question 1 applies). The Bank must set up a central control system (for example: only "just in time access", i.e. access on a strict individual basis; access on a "need to know" basis; in each case under the control of the Bank; "principle of dual control", in principle without the transfer of control competencies to external support staff; "least privilege") if the support of employees of a Cloud Provider, who was not appointed as an Agent, leads to Plaintext-Access to protected information of Bank customers. The Bank's criminal liability can be avoided if such a control system is adequately implemented, irrespective of the question of the Agent's position.

In summary: It can be confirmed, that the use of a Cloud Solution by Banks is lawful. The Bank can also use mature Cloud Providers if a Cloud Provider does not agree to the Bank's personal perimeter, as long as the Cloud Solution is sufficiently protected pursuant to the answers to questions 1 and 3 against disclosures by means of technical, organizational and contractual measures. Either way, the Bank must ensure the implementation of technical, organizational and contractual measures and require transparency on the part of the Cloud Provider. The Bank has to deal with the technical-organizational maturity of the Cloud Provider and understand how the Cloud Provider deals with data that is migrated by the Bank to its IT Infrastructure.

PART 1 BASICS

I. Reason and Subject

A. Reason for This Legal Opinion

1 The Swiss Bankers Association (SBA) has drafted a Cloud Guide on the use of Cloud Offerings by Banks and Securities Dealers. With regard to Banking Secrecy, the SBA asks the following specific questions:

a. Question 1: (a) Can a Swiss Bank use Cloud Offerings in light of Art. 47 Banking Act? (b) Is the answer different for foreign Cloud Offerings?

b. Question 2: (a) Can a Cloud Provider act as an "Agent" within the meaning of Art. 47 Banking Act, and is the disclosure of bank customer data to the Cloud Provider punishable under Art. 47 Banking Act in such cases? (b) Is the answer different for foreign Cloud Offerings?

c. Question 3: According to Art. 47 Banking Act, is it permissible for a Cloud Provider not appointed as an Agent to access secret information as long as this is purely for operational purposes (especially IT maintenance or support)?

2 LAUX LAWYERS AG would like to participate in the discussion of the SBA and has prepared the present Legal Opinion for this purpose. This Legal Opinion does not constitute an assessment of SBA's Cloud Guide.

3 LAUX LAWYERS AG is a law firm with specialized expertise in the intersection of law and information technology. The lawyers at LAUX LAWYERS AG have many years of experience in the financial industry (including in-house counsel experience at major Swiss Banks and global IT outsourcing providers). LAUX LAWYERS AG advises clients in the financial industry on IT issues as well as domestic and foreign Cloud Providers in dealing with Banks.

B. Subject

4 This Legal Opinion discusses the extent to which and the conditions under which a Bank may use Cloud Offerings. The analysis is limited to the criminal law aspects of Banking Secrecy (Art. 47 Banking Act) and is based on the three questions of the SBA. Other topics are not discussed in this Legal Opinion.[8] The terminology used in this Legal Opinion can be found in Appendix 1.

---

8 In particular, this Legal Opinion does not include a discussion of the FINMA Circulars (RS 2018/3 "Outsourcing - Banks and Insurance Companies" and RS 2008/21 "Operational Risks"), of data protection aspects, of restrictions imposed on a bank in the context of internal directives or to which the Bank has been committed under contracts with bank customers or third parties; aspects of authority access (e.g., BÜPF or other topics such as CLOUD-Act, authority access, etc.); of provisions of the Swiss Criminal Code (Art. 273 StGB etc.). Practical information on the implementation (e.g. comprehensive descriptions of a specific solution, discussion of individual technical, organizational or contractual measures or combinations thereof; notes on the process planning of a cloud migration by the Bank; catalogs of requirements a Bank should follow with respect to organizational aspects; requirement catalogs to cover compliance requirements; information strategies towards Bank customers) are only addressed marginally.

C. Protecting a Secret Means Protecting a (Possibly Extended) Perimeter

5 Anyone who keeps a secret for a third party must always endeavor not to disclose the secret to anyone who is not authorized to see it (an "outsider"). The keeper of the secret has to control everything in his or her sphere of influence (synonym: risk sphere). This means protecting the risk sphere against leaks, i.e. against any event in the context of which the secret could be revealed to an outsider. We refer to this obligation as a duty to secure the Bank's perimeter. Basically, the Bank must understand where its boundaries are. It must be able to define where the Bank begins and where it ends. At minimum, protecting a perimeter involves the following three aspects:

- the physical perimeter must be protected: buildings, etc. are to be protected against access by unauthorized persons.
- the logical perimeter must be protected: network and other IT Infrastructures must be protected against logical access by unauthorized third parties (hackers, etc.).
- the personal perimeter must be protected: in a collaborative economy no one works entirely on their own. A Bank must be able to define at all times where the Bank begins and where it ends. This is done by way of appropriate contracts with those persons and companies that support the Bank in its task.

6 From the point of view of the bank customer, the above translates into the following: The bank customer has a contract with the Bank as an institution and trusts that the Bank keeps information about the bank customer secret from outsiders. Furthermore, the bank customer expects and typically assumes that, within the Bank, confidential information may be shared among employees of the Bank, but at the same time the customer would also typically expect that, within the Bank, only those required to see information can actually access it ("need-to-know principle").

II. General Aspects Regarding Banking Secrecy

A. Legal Basis

1. Contractual Basis

7 Complementary basis: Confidentiality would be an ancillary obligation of the Bank towards the bank customer under the Swiss Code of Obligations (**CO**) even if their agreement was tacit with respect to this aspect. According to Art. 398 para. 2 CO, an agent is liable to the principal for the diligent and faithful performance of the business entrusted to him. In this context, the Bank is the agent entrusted with some of the bank customer's business (the principal). Thus, the entrusted Bank (the agent) has a legal obligation to maintain the confidentiality of the information pertaining to the bank customer (the principal). Information about the existence of a banking relationship, information about specific details of the relationship, and – obviously – information about the customer's assets – all of these aspects are subject to the bank customer's right to have such information protected. Art. 398 para. 2 CO also requires the Bank to safeguard the so-called "integrity interests" of the bank customer. This includes the bank customer's interest in having his or her personality rights protected in accordance with Art. 28 Swiss Civil Code (**CC**).

2. Reinforcement of the Contractual Protection under Art. 47 Banking Act

8 The resulting Banking Secrecy receives an additional layer of protection as a result of several provisions included in public law financial market statutes, the most prominent and most relevant in practice of which is Art. 47 Banking Act.[9]

9 In addition, data protection law and administrative law also reinforce Banking Secrecy (for example, Annex 3 to FINMA Circular 2008/21). This will not be discussed further here.

3. Additional Considerations

10 Banking Secrecy is primarily established under rules of private law (see para. 7 et seq.). Therefore, it is important to take account of what the bank customer expects with respect to the confidentiality of the information processed by the Bank. Bank customers expect the Bank to protect their perimeter (see para. 5). Under this condition, the bank customer agrees that the Bank processes particularly sensitive financial information relating to him or her. The efforts undertaken by the Bank must use state-of-the-art technology and the related processes must be established with care. However, the bank customer does not need to know which measures the Bank uses to protect its perimeter. Bank customers cannot and do not need to assess the usefulness of the measures undertaken by the Bank.

11 From the Bank's point of view, the Banking business is protected by constitutional guarantees, such as the right to economic freedom, and the guarantee of the Bank's property interests. The Bank may decide for itself which business it wants to pursue and how it wants to carry it out – as long as it complies with legal and regulatory requirements. The Bank freedoms that are protected by constitutional guarantees include the decision concerning which IT Infrastructures and which other IT-related setup the Bank wishes to use. It is not up to the bank customer to decide how the Bank organizes itself. That decision is reserved to the Bank and the Bank does not need to inform the bank customer of this – as long as it remains within the bounds of what is usually deemed to be expected and appropriate.

12 The Bank may also trust that the bank customer will not object to its internal organization as long as the Bank maintains appropriate measures to secure its perimeter. In this respect, the principle of trust applies. As long as the Bank takes appropriate protective measures, it may also assume that it has the implicit consent of the bank customer for arranging for the appropriate IT Infrastructures.

---

9 Similar penalties can be found, inter alia, in some other laws relevant to the Swiss financial market (Article 43 of the Federal Act on Stock Exchanges and Securities Trading (SESTA), Article 147 of the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (FMIA) and Art 148 para. 1 lit. k of the Federal Act on Collective Investment Schemes (CISA)). These rules will not be discussed further in this Legal Opinion.

13 In addition, recent legislative developments are of great importance: By no means does Banking Secrecy provide the bank customer with an absolute shield against disclosures that are not authorized by him or her.[10] In fact, the Banking Secrecy can be lifted without the consent and even contrary to the interests of the bank customer, for example, in tax matters.[11] The public interest in an internationally integrated financial system ("Level Playing Field")[12] may take precedence over the bank customer's interest to see his or her integrity and privacy protected. A corresponding assessment of recent legislation is important to determine whether the government has an interest in the enforcement of Art. 47 Banking Act.

B. Objective Facts of Art. 47 Banking Act

1. Introduction

14 Under Art. 47 Banking Act, disclosing a Banking Secrecy is a criminal act. "Disclosure" is the core concept of the rule. In the context of this Legal Opinion, the analysis is limited to this term. The other constituent elements – in particular the term "secret" – are sufficiently described in the standard literature.

15 There is no case law in Switzerland that would clarify the concept of "disclosure" in connection with Cloud Offerings in general. Therefore, further analysis is needed to determine and clarify whether the transfer of data to the IT Infrastructures of a Cloud Provider constitutes a "disclosure" within the meaning of Art. 47 Banking Act.

2. The Concept of "Disclosure" in Case Law and Doctrine

16 In a recent ruling, the Federal Supreme Court took the position that a disclosure only takes place once an outsider has actually gained knowledge of the information that was intended to be protected (i.e. the "secret").[13] Such knowledge is what, in this Legal Opinion, is referred to as Plaintext Access:

> *In dem von der Vorinstanz erwähnten BGE 142 IV 65 E. 5.1 hat das Bundesgericht erwogen, dass ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht. Es handelt sich hierbei um eine blosse Umschreibung des strafbaren Verhaltens, woraus – entgegen der Meinung der Vorinstanz – nichts zum Zeitpunkt der Vollendung der Tat abgeleitet werden kann. Vielmehr ist in dieser Frage der Lehre zu folgen, wonach die Tat vollendet ist, sobald ein Aussenstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält. Strafbarer Versuch wäre insbesondere dann anzunehmen, wenn der Täter Informationen für einen Dritten zugänglich gemacht hat, dieser aber vom Geheimnis noch keine Kenntnis genommen hat (DONATSCH/THOMMEN/WOHLERS, Strafrecht IV, 5. Aufl. 2017, S. 580 f.; siehe auch NIGGLI/HAGENSTEIN, in: Basler Kommentar, Strafrecht II, 3. Aufl. 2014, N. 36 zu Art. 162 StGB). Keiner der Mitarbeiter der B._____ Sagl nahm von den Zeichnungen, welche sich im*

---

10 BBl 1970 I 1944 et seq., 1161: "*Es muss hier gleich mit allem Nachdruck betont werden, dass das Bankgeheimnis nicht unbeschränkt gilt und keinen Deckmantel für Delikte darstellt. Artikel 47 des Bankengesetzes bestraft bloss die widerrechtliche Verletzung des Bankgeheimnisses*."

11 For example, since 2017, bank details have been automatically collected and exchanged between countries that have committed to apply the Global Standard for International Automatic Exchange of Information (AEOI). For details see below, para. 47 et seq.

12 BBl 2017 4913 et seq., 4935.

13 BGer 6B_1403/2017 of 8 August 2018, consid. 1.2.2; SJZ 114/2018 p. 453.

Altpapier befanden, Kenntnis. Ein Schuldspruch wegen einer vollendeten Verletzung des Fabrikations- oder Geschäftsgeheimnisses ist damit von vornherein ausgeschlossen. Der angefochtene Entscheid ist bereits aus diesem Grund aufzuheben.

17 In essence, the most recent case law summarized above clarifies that disclosure is a result ("Erfolg") that is required to complete the criminal act.[14][15] To put it differently, disclosure is a result without which the criminal act is not complete. This makes Art. 47 Banking Act an objective crime ("Erfolgsdelikt"). Disclosure thus means "making accessible" information that per se conveys meaning to the person seeing it (Plaintext Access), but only if the outsider actually gains knowledge of the information. The objective fact of Art. 47 Banking Act is not met if there is no Plaintext Access. And if there is no Plaintext Access, the reason why is not relevant (i.e. whether access has been absolutely impossible or whether it demonstrably has not taken place). For example, there is no disclosure if an unauthorized person temporarily has physical control over some storage media but does not have the means to read the data stored on the storage media.

18 The qualification as an objective crime ("Erfolgsdelikt") is not clearly supported by past doctrine[16] and case law[17] It is correct, nevertheless. As the Swiss Federal Supreme Court states, one must distinguish *the activities* that actually bring about a disclosure, or can bring about a disclosure, from their *effect or result* (disclosure as such[18]). The modern world requires this distinction.[19]

---

14 This does not include encrypted or anonymous information or information whose inspection still requires technical tools.

15 Example: If the keeper of the secret keeps a piece of paper that contains secret information 5 meters away from an unauthorized individual, there is no disclosure as long as the unauthorized person cannot read the text at this distance; if the unauthorized person has a telephoto lens through which he can read the text, there is a disclosure.

16 For example, Damian K. Graf, Zu den Anwendungsgrenzen des schweizerischen Strafrechts bei Geschäftsgeheimnisverletzungen, SJZ 112 (2016) 19 et seq., 197: *"Zunächst ist festzuhalten, dass es sich bei den Geheimnisverratsdelikten um schlichte Tätigkeitsdelikte handelt, ..."*, with further references. Andreas Donatsch, Strafrecht III, Delikte gegen den Einzelnen, 10th edition, Zurich 2013, 336; Olivier Weniger, La protection des secrets économiques et du savoir-faire [Know-how], Diss. Lausanne, Geneva 1994, 256; Georges Bindschedler, Der strafrechtliche Schutz wirtschaftlicher Geheimnisse, Diss. Bern, Bern 1981, 57 et seq. and 72. However, most recently for a qualification as an objective crime (Erfolgsdelikt) with respect to the professional secrecy of attorneys: Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (SAV), 13.

17 BStGer SK.2017.52 of 4 April 2018, consid. 4.2.2.: "*Umstritten ist, ob die Tat erst mit der Kenntnisnahme durch den Geheimnisempfänger oder bereits mit der Übergabe oder der Einräumung der Möglichkeit der Kenntnisnahme des Geheimnisses an Dritte vollendet wird (vgl. auch Urteil des Bundesstrafgerichts SK. 2016.14 vom 16. Mai 2017 E. 2.2.2). Das Bundesgericht hat sich dazu bislang, soweit ersichtlich, nicht direkt geäussert.*"

18 At least unclear: GIUSEPPE MUSCHIETTI, Wirtschaftlicher Nachrichtendienst – eine richterliche Perspektive, EIZ - Europa Institut Zürich Volume no. 157, Zurich 2015, 113 et seq., 135 et seq.: "*Die Straftat ist vollendet, sobald der Destinatär in der Lage ist, das Geheimnis - auch nur teilweise - zur Kenntnis zu nehmen.*"

19 The confusion about the correct qualification of the criminal provisions must be seen in terms of their historical developments. Until most recently, it may have been sufficient to focus on the Content Layer. The modern world, however, is disconnected and finer lines must be drawn to understand what "disclosure" means. Most recently, a legal scholar has put the problem as follows: "*Und was sind eigentlich Daten? Die meisten JuristInnen begreifen Daten von ihrem Inhalt (content) her, d.h. als Information. Sie denken semiotisch. Nur: die Digitalität kennt keine Semiotik. Sinnieren sie über Digitalität, tun sie das in den Kategorien der Hermeneutik. So wurden sie ausgebildet. Nur: die Digitalität kennt keine Hermeneutik. Verpassen sie die Idiosynkrasien der Digitalität? Lavieren bringt hier nichts: JA, vollends. Nicht einmal die Schlüsselfrage der Digitalität vermögen sie heuristisch zu fassen. Kein Wunder.*" Marc Amstutz at https://www.rechtimkontext.de/nc/veranstaltungen/veranstaltung/digitalverfassung-zwischen-staatlicher-und-zivilgesellschaftlicher-konstitutionalisierung/. Marc Amstutz writes this in the introduction to a presentation he gave and which was provided in the context of his research as published in AcP 218, 438 et seq. regarding the ownership of information (Marc Amstutz, Dateneigentum – Funktion und Form, AcP 218, 438 et seq.). The disconnect is also discussed by Marc Amstutz in Dateneigentum – Eckstein der kommenden Digitalordnung, Neue Zürcher Zeitung of 5 September 2018, 10. What this means: Digitization is a problem that requires a new look at the facts. Traditional doctrine may too easily result in wrong conclusions.

19 In addition, on the level of the activities that bring about a disclosure, a further distinction must be made. Past legal doctrine and case law have focused on the active performance of the criminal deed, for example, with respect to the following:

- **Direct communication of information**: The perpetrator has given a third party direct Plaintext Access to protected information. Example: Informing an expert about the facts in a lawsuit.[20] In the example, the recipient gains direct access to the protected information. Conversely, if – in addition to mere access to the data – an additional step must be taken to actually read the protected information, there is not yet any Plaintext Access.[21]

- **Creating a situation in which others can learn about protected information**[22]**:** Example: Sending a CD-ROM to a recipient who can read the contents of the CD.[23] In this scenario, the mere fact that an unauthorized person has access to data comprising proprietary information may be punishable[24] (but only if the outsider subsequently "opens" the data and reads the contents).

20 The offender may be punished based on the ideas he or she has formed of the subjective facts (Art. 22 para. 1 of the Swiss Criminal Code). However, punishment for attempting to commit a criminal act is only instituted if the person actually intended to disclose the information to the outsider. It is not possible (and thus not punishable) to make an unwilling attempt. In other words, a negligent attempt is impossible pursuant to the Swiss Criminal Code. Although scenarios involving active disclosures of protected information are conceivable, they are not the focus of this Legal Opinion. Rather, we seek to answer the question of whether a Bank can choose a setup that allows it to avoid being subject to punishment when using Cloud Offerings. Specifically, the question is what the Bank should do and what it should not overlook in order to avoid criminal liability when using Cloud Offerings. Therefore, below we focus on how breaches of banking secrecy by omission, i.e. breaches as a result of negligence, might be punishable.

3. Committing a Crime by Omission

21 Bank as Guarantor: Art. 47 Banking Act is designed as a misdemeanor ("Vergehen", Art. 10 para. 3 of the Swiss Criminal Code), both in the base scenario of the provision (intentional offense, Art. 47 para. 1 Banking Act) and in Art. 47 para. 3 Banking Act (offense as a result of negligence). The criminal act can therefore also be committed as a result of the failure to act ("by omission", Art. 11 para. 1 of the Swiss Criminal Code). Bank customers entrust the Bank with information about their personal situation in the course of the business relationship and trust that the Bank will protect this information through appropriate measures (para. 10). The obligation to take protective measures

---

20 OGer ZH UE140317 of 9 July 2015: *"Offenlegung von allfälligen Bankgeheimnissen gegenüber einem externen Privatgutachter [kann] tatbestandsmässig sein (...)".*

21 However, such event needs to be reviewed under the second aspect of the rule ("Creating a situation in which others can learn about protected information").

22 WOLFGANG WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), digma Schriften zum Datenrecht, Volume 9, Zurich 2016, p. 17 with further references.

23 OGer ZH SB110200 of 19 August 2016: "*Durch den Versand der CD an die Steuerbehörden und die Zeitschrift "Cash" hat der Beschuldigte dieses Geheimnis offenbart*".

24 With respect to Art. 321 StGB: BezGer Uster of 20 März 1996 (ZR 96/1997, 289, 294); STEFAN TRECHSEL, Schweizerisches Strafgesetzbuch, Kurzkommentar, Zurich 1997, StGB 320 N 8.

stems from the contractual arrangement between bank customer and the Bank (para. 7). Therefore, the Bank is a guarantor for the protection of the integrity interests of the bank customer.

22 Duties of Protection: Storing data in the IT Infrastructures of third parties does not constitute a breach of contract. The Bank must ensure sufficient protection of its perimeter (para. 5). This means that the Bank must provide sufficient safeguards that, in the ordinary course of events (i.e. during Normal Operation), effectively prevent unauthorized persons from gaining knowledge of the contents of the secret information (i.e. preventing Plaintext Access). If the Bank takes such safeguards it behaves as expected from the Bank customer's point of view (para. 5, para 10). If it fails to take such safeguards, then it acts contrary to its duties.

23 Ability to Control: The Bank has the ability to enforce safeguards before moving data to Cloud Solutions or, in the absence of such safeguards, not to use the Cloud Solutions ("Tatmacht"). It is sufficient if the Bank causes such safeguards to be taken. The safeguards can be taken by the Cloud Provider. If this is the case, the Bank should document the safeguards that are taken by the Cloud Provider. The documentation made available to the Bank must cover the entire Cloud Offering and describe in sufficient detail how the Cloud Provider ensures that the Bank's data is protected. Specifically, it must detail how the Cloud Provider protects data against unauthorized disclosures. Based on this documentation, the Bank must be able to understand whether the data migrated to the foreign IT Infrastructures is adequately protected. The documentation must serve this purpose. The Bank does not need to compile this documentation on its own; the Cloud Provider must provide it. In other words, before data is migrated to the IT Infrastructures of the Cloud Provider, it is up to the Bank to verify how the transferred data will be protected. The Bank must recognize in advance and, if necessary, avoid excessive threats to the confidentiality interests of its customers. In other words, the Bank has a criminally relevant ability to control inherent risks.

24 Hypothetical Causation: Today, the technical capabilities of the cloud industry are quite advanced. How such protection may look is described below in greater detail (PART 2, para. 64 et seq.). Even if the protective safeguards that have been put in place leave a theoretical residual risk of disclosure and that third parties will gain unauthorized Plaintext Access to the data migrated to the IT Infrastructures of the Cloud Provider, this does not mean that such access will take place during Normal Operation. Depending on the selected Cloud Offering, it can even be shown that Plaintext Access to secret information is completely excluded during Normal Operation. In other words, by carefully selecting which Cloud Offerings to use, the Bank can control what data it protects and how. If it fails to take the measures available to it and if subsequently a prohibited disclosure occurs, the question arises as to whether the disclosure could have been avoided by the Bank (e.g. by more carefully aligning with the Cloud Provider). If the Bank has not been diligent in choosing and controlling the Cloud Provider, the omission could be relevant from a criminal law perspective and could be construed as a cause of the disclosure. However, the Bank is not responsible for events it cannot anticipate with sufficient certainty. Access by unauthorized third parties would be such an event. Accordingly, in the event a third party unlawfully overcomes the protective measures, then that third party may, of course, be subject to punishment. However, the Bank would not be liable under Art. 47 Banking Act, provided the data sets in question were protected by appropriate safeguards that generally prevent such disclosure. In the same way, if the Cloud Provider declares bankruptcy and certain disclosures of secret information cannot be avoided, this does not constitute a punishable

breach by the Bank under Art. 47 Banking Act. Likewise, access by a particular authority to protected data is beyond the Bank's control. These examples show that the Bank is responsible only for the measures it should have undertaken to prevent risks that could be expected during the Normal Operation of the Cloud Solution.

25 Reasonableness Standard: The measures to be taken by the Bank to protect the perimeter must be reasonable for the Bank. There is little discussion in the doctrine about the level and quality of measures that have to be taken by the Bank. It would be unreasonable to ask the Bank to guarantee that Plaintext Access be absolutely impossible. There is no a priori breach of Art. 47 Banking Act merely because, from a purely technical point of view, there is a theoretical possibility that someone other than the Bank can access the secret – as long as measures are in force that normally prevent unauthorized third parties from gaining Plaintext Access to the secret information. For the sake of comparison, the Bank would not have such an obligation with regard to data stored on its own IT Infrastructures either. The measures implemented must solely, but at minimum, comply with current state of the art technology. To the extent the Bank does not procure for such measures, it exposes itself or its executives (or employees acting on its behalf) to a criminally relevant risk.

26 Conclusion: The above statements mean that a Bank (that is, the persons acting on its behalf) that ensures sufficient technical and organizational protection against unauthorized access is not liable to prosecution under Art. 47 Banking Act. The use of Cloud Offerings that are mature enough to provide for such adequate protection is allowed by a Bank under Art. 47 Banking Act. If the Bank fails to take appropriate measures to protect itself and if, as a result, Plaintext Access to protected information (i.e. a disclosure) is gained by an unauthorized individual, the persons making the decisions can be prosecuted – unless the Bank can rely on a safe harbor argument under which Plaintext Access occurring in the context of the Cloud Solution are justifiable (see para. 30).

C. Subjective Facts for Art. 47 Banking Act

27 A breach of Banking Secrecy is punishable if the rule has been violated either intentionally or negligently. There are no intentional or negligent offense if the Bank's governing bodies conclude, based on an informed decision, that the technical IT Infrastructures they have chosen effectively protect against disclosure of confidential information to unauthorized outsiders.

28 No IT Infrastructure completely protects against unauthorized access. If a Bank's officers and employees are aware that there are small residual risks to unauthorized disclosures, they will not be deemed to be guilty as long as they have procured for protective measures to be applied by the Cloud Provider.

29 These measures, if documented, are confirmation for the defense that the Bank's officers or employees are not guilty of negligent behavior (or omissions). Persons acting on behalf of the Bank are liable for negligence only if they fail to comply with the Bank's duty of diligence. Here, too, it is crucial to be able to demonstrate that the Bank has arranged for effective technical and organizational measures to prevent the unauthorized disclosure of the protected information. The Bank must ensure the confidence of the security measures by implementing meaningful documentation and effective controls.

III. Analysis of Art. 47 para. 1 Banking Act

A. Introduction

30 Art. 47 Banking Act is a special offense, i.e. perpetrators are limited to the explicit and exhaustive list of persons within the Bank's risk sphere (for example, bodies and employees). Since 1971, disclosure of a banking secret has been a criminal act if the disclosure is made by an Agent ("Beauftragter") of the Bank. The aim of this provision was to allow Banks to use Outsourcing Services in a meaningful way.[25] The materials clarify that the IT Infrastructure of providers offering services to Banks should become subject to criminal liability with that amendment.[26] Since Agents belong to the circle of the punishable persons, the "disclosure of customer relations to Agents"[27] by the Bank is lawful.[28] If the Agent is a legal entity, the individuals acting on behalf of that legal entity are subject to criminal liability according to Art. 47 para. 1 lit. c Banking Act.

31 For their services, Cloud Providers also use IT Infrastructures such as data centers. As a result, Cloud Providers may qualify as Agents. It must then be determined whether Cloud Providers actually are "Agents" within the meaning of Art. 47 para. 1 lit. a Banking Act.

B. Cloud Providers as Agents

1. Interpretation Based on the Text and Legislative History

32 The Swiss legal concept of an Agent is very vague. This vagueness was intentional. The German text of the law uses the term "in seiner Eigenschaft als ... Beauftragter", the French text "en qualité ... de mandataire", and the Italian version "nella sua qualità di membro di ... mandatario". The historical interpretations reveal that the term "Agent" (Beauftragter, mandataire, mandatario) does not have a special legislative limitation as to which service offerings are covered by the term. Even providers of pure data center services are covered, as was the explicit intention of the Federal Council preparing the explanatory document for the 1971 legislative amendment (see above, para. 30). The legislature generally wanted to allow external third parties to be included in the risk sphere of the Bank. It did so because collaboration was becoming standard in the business world. Banks should be permitted to engage in shared responsibilities with specialized providers when serving

---

25 BSK BankG-STRATENWERTH, Art. 47 N 7: "*Das wird man dahin verallgemeinern dürfen, dass die Bank Dritte jedenfalls dann in den Kreis der Geheimnisträger einbeziehen darf, wenn dies einem ernstzunehmenden Interesse an der Optimierung ihrer Leistungen oder an der Senkung ihrer Kosten entspricht. Die in solchem Rahmen erfolgende Weitergabe personenbezogener Daten dürfte in aller Regel auch im wohlverstandenen Interesse des Bankkunden liegen, um dessen Schutz es geht.*"

26 BBl 1970 I 1144 et seq., 1182: *"Mit der Unterstellung des Beauftragten sollen insbesondere auch Rechenzentren erfasst werden, die von Banken mit der elektronischen Datenverarbeitung betraut werden."*

27 BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, in: Zobl/Schwob/Geiger/Winzeler/Kaufmann/Weber/Kramer (publisher), Kommentar zum Bundesgesetz über die Banken und Sparkassen, 23. edition, Zurich etc. 2015, Art. 47 N 369: "*Die Preisgabe von Kundenbeziehungen an Beauftragte ist somit i.S.v. Art. 32 StGB grundsätzlich erlaubt. Die Erläuterung in der Botschaft ("insbesondere") lässt erkennen, dass der Wortlaut von Art. 47 Abs. 1 BankG insoweit für Entwicklungen der Zukunft nicht nur offen gehalten, sondern auch mit Absicht so formuliert wurde.*"

28 BEAT KLEINER/RENATE SCHWOB, in: Bodmer/Kleiner/Lutz (publisher), Kommentar zum schweizerischen Bankengesetz, Zurich 1996, BankG 47 N 102; URS ZULAUF, Bankgeheimnis und historische Forschung, ZSR 113 I (1994), 115; PETER HONEGGER/THOMAS A. FRICK, Das Bankgeheimnis im Konzern und bei Übernahmen, SZW 1996 6.

bank customers, even if such arrangements are not readily apparent to bank customers. The proximity of a Cloud Provider to a provider of data center services is obvious, as a Cloud Provider also offers IT Infrastructures for use by its customers. The legislative text and history are clear: Cloud Providers can be understood as falling under the term “Agent” according to a literal interpretation. This interpretation still appears adequate today and does not need any correction.

2. Systematic Interpretation

33 Of the numerous people who work at a Bank, many have access to customer-related data, and in some cases, they may be in a position to gain knowledge of protected secrets. The scope of Art. 47 Banking Act extends to all persons who work at a Bank or who are contracted by the Bank. Agents are treated as part of the Bank’s overall workforce.[29] Other criminal laws protecting secrets under Swiss law (e.g. Art. 321 of the Swiss Criminal Code) use the term "auxiliary". The entire workforce employed by the respective keeper of the secret is subject to criminal liability. Although the Banking Act employs different terminology (using the terms "employee" and "Agent"), Art. 47 Banking Act has the same objective. In Art. 47 Banking Act, too, the definition of who is subject to criminal liability is based on a functional understanding. Anyone who works at or with a Bank within the framework of what is customary, socially accepted and in line with bank customers’ expectations today is subject to punishment for breaches (para. 10). The criminal provisions protecting secret information, whether they use the term “auxiliary” or a similar concept (such as “Agent”), are designed to enable a viable method of operating from a business perspective. Such legislative design[30] is apparent in other concepts of substantive Swiss law, more precisely in the rules Art. 68 CO, Art. 101 CO, and even in Art. 398 para. 3 CO and Art. 399 para. 1 CO (substantially confirming Art. 101 CO, at least in essence).

34 Therefore, from a functional perspective, Agents can be persons that collaborate with the Bank in such a close manner that it is useful, reasonable, and customary to give them Plaintext Access to protected information on an as-needed basis. In a modern economy based on a division of labor, providers of IT services, such as Cloud Providers, may be such persons.

3. Teleological Interpretation

35 The teleological interpretation does not go much further than the historical interpretation: lawmakers wanted to enable Banks to involve external providers of IT services in duly justified cases. Also, with regard to the teleological element, Cloud Providers can be appointed as Agents.

4. Other Interpretative Considerations: Functional Concept of Auxiliaries and How This Relates to the Implicit Consent of the Bank Customer

36 From a functional point of view, all persons mentioned in Art. 47 Banking Act are members of the same risk sphere (i.e. the sphere of the Bank to which they belong or for whom they act as Agents). Within this risk sphere, all those who work together in a collaborative manner must be able to trust

---

29 KLEINER/SCHWOB/WINZELER (footnote 27) Art. 47 N 360.

30 The secrecy rules (Amtsgeheimnis), which do not contain a clause regarding auxiliary persons, should be amended to include such a clause in the context of the legislative work being carried out with respect to the information protection law; see BBl 2017 2953 et seq., 3077 et seq.

each other. In a modern economy in which work is divided, collaboration involving the sharing of secret information is not only necessary but socially accepted as well. A criminal rule subjecting all members of that risk sphere to the same criminal sanctions reinforces and strengthens that sphere of risk and trust. As a result, many individuals may be "parallel" keepers of the secret.

37 To the extent that such parallelism of many members of the Bank's workforce corresponds to what is or can be expected, one can also assume that the bank customer has given his or her implied consent to it (para. 12). The scope of such consent cannot exceed the bank customer's level of expectation, though. Such consent covers behaviors that bank customers could and should expect.

5. Conclusion: Cloud Providers Can be Appointed as Agents within the Meaning of Art. 47 para. 1 lit. a Banking Act

38 The interpretation by means of various methods leads to the conclusion that Cloud Providers can be appointed as Agents within the meaning of Art. 47 para. 1 lit. a Banking Act. This means that if the Bank has appointed the Cloud Provider as an Agent, the Bank may exchange secret information with that Cloud Provider and give it Plaintext Access. This conclusion can be referred to as a privilege to exchange information between Banks and Cloud Providers.

C. Establishment of Foreign Agents

1. Introduction and Challenges

39 So far, the prevalent doctrine[31] is that the privileging effect (see para. 38) does not apply to a foreign Cloud Provider.[32] This will be clarified below.

40 The discussion needs to be conducted in light of the fact that an individual who has been appointed as an Agent and makes a relevant disclosure contrary to Bank's instructions would have to be prosecuted abroad. Although Art. 47 Banking Act has been qualified as an objective crime by the Federal Supreme Court, there is little agreement in the doctrine as to whether such criminal acts conducted abroad are definitely punishable under Swiss law. Art. 8 para. 1 of the Swiss Criminal Code is relevant here.[33] Either way, if a perpetrator who acted abroad does not voluntarily enter

---

31 KLEINER/SCHWOB/WINZELER (footnote 27), BankG 47 N 371: "*Da im Ausland domizilierte Beauftragte trotz theoretischer Strafbarkeit dem Arm der schweizerischen Strafbehörden praktisch entzogen sind ("Over the border means out of control"), darf die Bank Aufträge, die zur Preisgabe von Kundenbeziehungen führen, nur dann ins Ausland erteilen, wenn dafür gewichtige Gründe sprechen wie z.B. beim Anschluss an ein internationales Zahlungssystem.*"; same opinion: DAVID SCHWANINGER / STEPHANIE S. LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11 March 2013, N 31; URSULA WIDMER, Kurzgutachten für die Schweizerische Informatikkonferenz SIK betreffend die Nutzung von Cloud Services mit Rechtswahl von irischem Recht und Gerichtsstand Dublin durch die schweizerische öffentliche Verwaltung, 2012, 7.

32 Different: CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (SAV), 1 November 2018, p. 21, fn. 50, with reference to BezGer ZH GG150233 of 18 November 2015, consid. II.2.5.3. for the medical confidentiality in the sense of Art. 321 StGB: «Bei einem durch eine kleine Arztpraxis ohne Sekretariat beigezogenen auswärtigen Schreibbüro handle es sich um eine Hilfsperson, ***woran auch der Umstand nichts ändere, dass das Schreibbüro seine Arbeiten nicht in der Schweiz, sondern in Deutschland verrichtete.»***

33 In detail for the criminal law provisions in acts of digital disclosure DAMIAN K. GRAF, Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext, SJZ 112/2016, 193; SCHWARZENEGGER/THOUVENIN/STILLER, (footnote 32) p. 35 et seq.;

Switzerland or if the foreign state fails to extradite him or her, the prosecution would have to be conducted abroad. However, the disclosure may not be punishable in the relevant country or the perpetrator may be able to avoid punishment due to the concrete circumstances abroad.[34] These summary statements show that criminal law protections to protect bank-client secrecy may be reduced or even fully eliminated.

41 For this reason, a legal assessment would have to be conducted to determine if it is still possible for the Bank to assert sufficient control over the Cloud Provider, despite the reduction in or elimination of the criminal law protections. If sufficient control were affirmed, then the privileging effect (see also para. 38) would still apply.

42 This argument has been possible since 1971. Yet no Bank has decided in practice to avail itself of this justification to migrate data with banking secrecy relevance to a data center, for example, in India. Is it worth scrutinizing the text of Art. 47 Banking Act, which has remained unchanged since 1971, and its reception over the past 50 years? The answer is yes. While the law has not changed, the environment has.

2. Analysis of Art. 47 para. 1 Banking Act

a) Interpretation Based on the Text

43 The text of Art. 47 Banking Act does not distinguish between the domestic and foreign employees, bodies or agents, etc. of a Bank. According to the grammatical interpretation, the domestic and the foreign Agents of a Bank must be treated equally. Any other conclusion would violate Art. 1 Swiss Criminal Code ("nulla peona sine lege").

b) Interpretation Based on the Legislative History

44 When the concept of the "Agent" was introduced in Art. 47 Banking Act in 1971, possible issues of foreign implications related to Agents (or data center services) were not specifically discussed. Under the 1934 legislation in 1934, the stated goal of the Banking Secrecy legislation is to prevent data from being accessed by other states. In its dispatch to Parliament accompanying the revision of the Banking Act (1970), the Federal Council stated[35]:

> *1934 hat der schweizerische Gesetzgeber es für notwendig gehalten, die privatrechtliche Pflicht des Bankiers zur Verschwiegenheit durch eine Strafandrohung in Artikel 47 des Bankengesetzes zu verstärken. Bei den Beratungen über diese Bestimmung wurde erwähnt, dass sie sich nicht nur gegen die eigentlichen Verletzer des Bankgeheimnisses, sondern auch gegen "ausländische Spionage" richte. Es ging in der Tat darum, wirksam gegen die mannigfachen Versuche der totalitären Regime jener Zeit anzukämpfen, ihre Devisengesetzgebung, die oft auf Enteignung hinauslief, in der Schweiz zur Anwendung zu bringen und die Hand auf das in unsern Banken deponierte Vermögen der aus politischen oder rassischen Gründen verfolgten Personen zu legen. Der schweizerische Gesetzgeber wollte daher den Schutz der Persönlichkeit gegen Massnahmen verstärken, die unsere öffentliche Ordnung verletzen. Bankmoral und Bankrecht, wie die Schweizer sie für sich selbst entwickelt hatten, sollten auch für die Ausländer gelten.*

---

34 For example GRAF (footnote 33) 19 et seq..: "*Angesichts des wenig verbreiteten Schutzes von Bankkundeninformationen im Ausland steht die Voraussetzung der Reziprozität einer Verfolgung und Verurteilung wegen der Verletzung von Art. 47 BankG regelmässig entgegen.*"*;* with reference to: JÖRG SCHWARZ, in: Jürg-Beat Ackermann/Günter Heine, Wirtschaftsstrafrecht der Schweiz, 2013, §19 N 112.

35 BBl 1970 I 1144 et seq., 1161.

45 The historical consideration of lawmakers' intentions provides a different view of foreign Agents than what is indicated by the text of the law. Since then, the Banking Act has been revised several times and was recently adapted in line with the public interest to an internationally integrated financial market system. This contemporary view will be deepened in the context of a systematic consideration. As a result, lawmakers' intentions 80 years ago are less relevant in the current environment.

c) Systematic Interpretation

46 As a result of the latest legislation, Switzerland has distanced itself considerably from lawmakers' intentions in 1934:

47 By participating in the Global Standard for the International Automatic Exchange of Information (AEOI), Swiss Banks have been providing Swiss authorities with relatively detailed information on foreign Bank customers since 2017, so that such information can be forwarded abroad. Switzerland wants to participate in the international financial market system ("Level Playing Field", para.13). Over the course of several iterations from 2015 to 2018, the Federal Counsel has presented the basis for this to the Parliament for consultation. The first AEOI Act has been in force since 2017. Switzerland has exchanged information about financial accounts with partner states under the AEOI since 2018.

48 Switzerland has signed an international treaty with the United States to facilitate the implementation of FATCA ("US Foreign Account Tax Compliance Act") and has issued a corresponding Swiss FATCA Act. As part of this FATCA agreement, Swiss Banks report account information directly to the US tax authorities with the consent of the clients affected. If consent is not given, an anonymous, aggregated message will be sent instead of the account information. On this basis, the US tax authorities may request the disclosure of certain client and account information, as provided for in the US-Switzerland double taxation agreement.

49 These recent developments make clear the importance of lawmakers' historical intention. Under a system such as the AEOI, Banks transmit standardized, aggregated information of bank customers without prejudice to foreign countries. This is in many ways important for the question as to whether a foreign Agent may be established by a Swiss Bank: the protection interests pursued by lawmakers in 1934 have been overridden by the AEOI, since participating states no longer need to make a detour via an Agent (after passing through restrictive procedures) to be able to access the same information. If the foreign state needs more information than what has already exchanged under AEOI, it can contact the Agent via its law enforcement authorities to obtain further information directly (without involving Switzerland's authorities). But even in Switzerland, Bank Secrecy does not prevent law enforcement authorities who pursue crimes of a certain intensity from accessing such information. Switzerland would in all cases provide legal assistance to the foreign state for such investigations. If employees of the Agent break secrecy laws, they could be prosecuted abroad under local law (depending on the legislation there); depending on the opinion, the foreign criminal act could also be prosecuted in Switzerland.[36]

---

36 See above para. 40 with further references.

50 These considerations are especially important when assessing Art. 47 Banking Act as a criminal provision. Art. 47 Banking Act represents a statutory reinforcement of the contractual protection of secrecy (para. 7). It specifies the offenses that are subject to criminal prosecution, expressing the state's right to prosecute such offenses. It would be contradictory if the same state that transmitted data abroad without any preconditions and across the board for all banks (and their customers) in the framework of the automatic exchange of information were to subject data transmissions that are much narrower in scope and which have been stored in technically secure IT Infrastructures to criminal liability (without specifically stating this in the elements of the offense). As a result, the historical interpretation (para. 44) is no longer decisive for this interpretation.

51 In the framework of the systematic interpretation, it should also be noted that the opinion has been voiced recently that in the area of attorney-client privilege foreign agents may also be legally included in the attorney's risk sphere and that it would not represent a breach of attorney-client privilege if such foreign agents were granted plaintext access to secret information.[37]

d) Teleological Interpretation

52 For the teleological interpretation, see the statements in para. 35. Art. 47 Banking Act is intended to allow banks, for objective reasons, to position themselves as required in an economy based on a division of labor. The Bank should be able to include service providers in its risk sphere for this purpose. Because of the international nature of the Cloud Offering now, the teleological argument leads to the logical conclusion that the use of foreign Agents should be permitted.

53 At any rate, it is clear that Art. 47 Banking Act is not intended to offer protection for domestic Cloud Providers. As a criminal provision, it would not be suitable for this purpose; a corresponding connotation would have to be rejected in the interpretation.

e) Conclusion

54 The assessment of the above interpretations leads to the clear conclusion that banks may also appoint foreign service providers as Agents within the meaning of Art. 47 Banking Act.

---

37 SCHWARZENEGGER/THOUVENIN/STILLER, (footnote 32), p. 21, 27 et seq.

PART 2 IMPLEMENTATION OF APPROPRIATE PROTECTIVE MEASURES

I. Conclusions Based on Considerations Related to the Objective and Subjective Facts

A. Introduction

55 The considerations regarding objective and subjective facts (above, see para. 14 et seq.) show that Art. 47 BankG should be assessed as a non-genuine omission offense in the event of negligent conduct (para. 21). Both in its role as a guarantor and in order to avoid a charge of negligent conduct, the Bank is obliged to exercise care when selecting the Cloud Provider, to anticipate foreseeable risks and to have the Cloud Provider indicate the measures with which it will protect bank customer data against unauthorized access. If, after a careful assessment, the Bank comes to the conclusion that the measures indicated to it by the Cloud Provider will not lead to any disclosures during the foreseeable course of Normal Operations (including disclosures to the Cloud Provider's employees), or if, on this basis, it includes the Cloud Provider in its risk sphere as an Agent on a contractual basis (as a result of which, Plaintext Access by Cloud Provider employees is permitted), then the Bank is not breaching its position as guarantor and nor can the bodies and employees of the Bank be punished for a negligent offence.

56 A Bank that ensures adequate technical and organizational protection to prevent unauthorized parties from gaining knowledge of the secret information during the ordinary course of business cannot, from an assessment standpoint, breach banking secrecy on the basis of objective elements. **Adequate protection** means that **sufficient measures** to prevent access by unauthorized third parties must be taken effectively. Such measures are sufficient if, during the course of normal operations (ordinary course of business) they generally prevent unauthorized parties from gaining knowledge of the secret information ("Plaintext Access").

57 The Bank must understand the extent to which it, through documented measures, maintains control over the data that has been migrated to the external IT Infrastructures (obligation to protect its own perimeter, para. 5), as the Bank can only control what it also understands.

58 If the Bank proceeds in this manner, it can document that it has *complied with its contractual obligation to act as the guarantor* and that it has not acted *negligently*.

59 The Bank must ensure that it has internal structures and internal employees, both in the procurement process and during operations, maintain control of the exchange with the Cloud Provider. This means that internal employees must occupy new areas and undergo some retraining for the required skills ("skill shift").

B. Conclusions Based on the Considerations Related to the Agent's Position

60 The law does not specifically state how an Agent acquires its privileged position. The status of an Agent may be acquired by law, i.e. automatically when the contract is concluded. Alternatively, the Bank may need to explicitly establish the Agent as such. In the second alternative, the provider may become an Agent only after the Bank has duly integrated it in its sphere of risk, namely by means of a contract establishing specific safeguards.

61 The functional considerations relating to the limitations inherently expressed by the bank customer's tacit or implied consent are of relevance in deciding which alternative is the law. In particular, the Bank at all times must be able to determine the boundaries of "where the Bank begins and where it ends". To this end, the Bank must be able to document that its use of the Cloud Provider as an Agent (with Plaintext Access) is both necessary and does not result in a loss of control.

62 In particular, the following points are of relevance:

- Agreement is necessary: In our opinion, an explicit integration in the Bank's sphere of risk is required. Such integration requires explicit agreement. Only if such integration, by means of an explicit agreement, occurs are the limitations inherently expressed by the bank customer's tacit or implied consent reflected. Conversely, a Cloud Provider would not have the role of Agent if the Bank has not explicitly integrated it in its own sphere of risk. Absent an agreement, the Cloud Provider also would not be able to anticipate that its employees might be subject to criminal sanctions.

- Definition of risk spheres: The keeper of the secret (i.e. the Bank) is responsible for implementing measures that prevent the disclosure of the secret. Only with such measures, secured by an agreement between the Bank and the Cloud Provider, will the Bank be in line with the implicit expectations of the Bank's customers. It is legitimate for the Bank to trust other people within its own sphere of risk (this sphere of risk includes Agents).[38] To this end, however, the risk sphere must be defined. The definition of the risk sphere requires an agreement imposing obligations on the Cloud Provider to take sufficient technical and organizational measures.

- Assessment of the information disclosed to the Agent: In order to determine the required measures, the Bank must take into account the information that is disclosed to the Cloud Provider. For particularly sensitive information, the Bank should enforce a more restrictive regime (e.g. with respect to the need-to-know principle) than for other, less relevant information.[39]

63 Therefore, it is clear that not only purely formal criteria[40] but also content-related and functional criteria determine whether an Agent is lawfully appointed as such. It would not be enough if the Bank merely stated that the Agent is subject to "the criminal liability of Art. 47 Banking Act". Rather, through the protective measures arranged for in the respective agreement, the Bank must be able to confirm that the information to which the Agent may have Plaintext Access is still under the Bank's control. Control also requires an in-depth understanding on the part of the Bank about the procedures and measures established by the Cloud Provider because a Bank can exercise control only if it also understands how the setup of the Cloud Provider works. The Cloud Provider will need to provide adequate documentation to the Bank for this purpose.

---

38 SCHWARZENEGGER/THOUVENIN/STILLER, (footnote 32) p. 21.

39 DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, OR 328b N 57.

40 Rightfully so OGer ZH UE140317 of 9 July 2015 i.S., consid. 6: "*Allein die Tatsache, dass eine Person zur Bank ein Auftragsverhältnis unterhält, kann nicht genügen, um die Bank zur Weitergabe von Geheimnissen zu ermächtigen (compare Stratenwerth, ibid., N. 7 to Art. 47 BankG).*".

C. Scenarios without Plaintext Access

1. Preliminary Remarks

64 As long as the Cloud Provider is not formally appointed as an Agent, the Cloud Provider and its employees are considered unauthorized outsiders. However, this does not mean that the Bank cannot use Cloud Offerings. As the following will show, mature Cloud Offerings may be used by the Bank. In this context, a mature Cloud Solution is one in which well-established technical and organizational measures effectively prevent disclosures from actually occur.

65 Accordingly, while contractual measures are necessary for the formal appointment of the Agent, the scenario discussed here will be built mainly on the basis that certain technical and organizational measures are available. Interestingly, the measures discussed here will probably, at least in many aspects, not differ significantly from the technical and organizational measures required for the formal appointment of a Cloud Provider as an Agent – the main difference being that the Cloud Provider is not established as an Agent.

66 If the relevant data is adequately protected against access by unauthorized third parties, there will be no criminally relevant disclosure. There is no disclosure if the Bank, as the keeper of the secret, has required the Cloud Provider to apply protective measures that are at least state-of-the-art. Below we discuss the role of the solution design of the Cloud Solution in general. The solution design allows the Bank to use the Cloud Solution even if the Cloud Provider has not been formally appointed as an Agent. We identify usage scenarios and explain the extent to which possible variations in the service model (IaaS, PaaS, SaaS) lead to distinctions in the legal analysis:

2. Analysis of the Different Service Models

a) Pure IaaS Offerings

67 In a pure IaaS offering, the Bank uses the Cloud Provider's IT Infrastructures – this means essentially buildings, servers, layers of virtualization, and storage components. These resources are not used in isolation, but rather are the Base Components[41] based on which the Bank can procure and use Virtual Machines. The user experience for users of these Virtual Machines (as they are generated by means of Base Components procured from the Cloud Provider) does not differ significantly from the previous user experience (IT Infrastructures at the Bank's premises). Of course, the technical methods of presenting them to the end user do differ.

68 With an IaaS model, it is important to note that the Base Components used by the Cloud Provider are managed automatically by the Cloud Provider. This is done by means of central control systems that enable the Cloud Provider to manage the Base Components that are made available on a large scale. It is a core approach for the Cloud Provider to run and manage the Base Components with an appropriate effort and to a high degree of automation. In other words, the Bank benefits from

---

41 We establish "**Base Components**" as a defined term (see Annex) to permit a distinction between (a) the bare metal machinery plus the software artefacts a Cloud Provider deploys in its data centers and (b) the **Virtual Machines** and (c) the **Tenants**. While (a) is the real-world technology, (b) is what (a) is presenting. Tenants (c) are logical arrangements to organize how the Virtual Machines (b) actually deploy effects to a user.

the Cloud Provider's IT Infrastructures in the same way that other customers do, and the Cloud Provider provides them according to uniform methods (i.e. all customers benefit from these management activities in the same way). The Cloud Provider does not expect to provide the Bank with customer-specific provisioning.

69 The Cloud Provider operates the central control systems in such a way that all Base Components (to the extent they involve software) are automatically updated at all levels of the IT Infrastructures (or, for a selection of the Base Components, on the basis of criteria that are defined in the abstract, and not in a customer-specific way: version number, age of the hardware, etc.). In other words, management is also provided uniformly and in an anonymized, non-dedicated manner. The central control systems thus enable more efficient oversight of actions to maintain and improve the overall cloud solution.

70 Why is this relevant? With this approach, the Cloud Provider's resources are not managed directly by humans (meaning, for example, human manipulation on a physical machine), manually or in a customer-dedicated manner – but in an automated, anonymous, uniform and non-dedicated manner for the entire customer base in the same way. This approach is what is usually referred to as "hyperscale". Other than what may be true for small IT Infrastructures, cloud solutions built on a hyperscale approach are necessarily managed anonymously. While humans (the Cloud Provider's personnel) still operate the central control systems, the focus is more on the control of *management criteria* (the criteria according to which machines perform certain tasks) than the performance of customer-specific management tasks.

71 The administration of IT Infrastructures with a hyperscale approach is reflected in procedures (i.e. technical and organizational measures) that promote anonymity, the most common of which are detailed below:

- Approval processes ensure that, at no time, can a single employee have uncorroborated access to Base Components, or to a system controlling these (i.e. to the central control systems, or a portion of them). Access to the central control systems must be authorized by a manager who has approval authority. The manager should be set up to have this approval role for this dedicated purpose only; the manager should not otherwise cooperate with the employee requesting access. In addition, approval roles should be set up to be under constant change so that the employee requesting approval cannot predict who will be in the approver role. Such approval processes also promote anonymity within the teams of the Cloud Provider, minimizing, if not ruling out, conflicts of interest and collusion to the detriment of a particular customer.

- Of course, the request to access certain Base Components, or the central control systems, as made by the requesting employee must be based on plausible grounds.

- If access is granted to the requesting employee such access should be given only for the duration needed by the employee for the purposes stated in the approval request ("just in time" access). The management rights granted to the requesting employee should be limited to what is necessary as per the access request, and to what is appropriate for the purposes of the access request ("just enough" access).

- All activities performed during the period when access rights have been granted and the entire request process should be recorded in logs.

- Other than such limited access to Base Components, access to Tenants is not anticipated.

72 Such an organizational methodology, as backed by technical implementations, will limit the overall likelihood that, during Normal Operation, a Cloud Provider's employee could access one the Bank's Virtual Machines and the data on it.

73 But the IaaS model is not solely about organizational measures. Technical characteristics further operate to the benefit of the customer in terms of Tenant isolation. The central control systems involve software with a dedicated functionality. Therefore, personnel using it to access certain Base Components can do so only as permitted by the functionality offered within the central control systems. Where the central control systems do not permit certain types of access, there is an additional layer of protection. The purpose of the central control system is to configure and update the Cloud Provider's Base Components. Conversely, it is not intended to be used to access the Tenants of individual customers, i.e. of Banks. Accessing the Bank's Tenant as such would require other systems and, more importantly, other permissions (and require the customer's consent – with this requirement also incorporated in software routines that support the requirement).

74 With an IaaS approach, the Bank is free – but also obliged[42] – to independently define the setup within the Virtual Machine: It selects the specific software configuration (operating system and application software) on the Virtual Machine and defines the data models it desires. If the Bank loses the access data for the Virtual Machine or for the applications running on it, the Cloud Provider in the hyperscale model cannot help the customer initiate recovery measures. The customer then has to go through these recovery measures on its own.

75 In addition, with the IaaS model it should be noted that, of course, the overall system is coordinated by the Cloud Provider. This leads to a layered authority model:

- The Cloud Provider can be said to provide the top-level administrators[43].

- The customer (i.e. the Bank) provides the second-level administrators[44]: Should an employee of the Cloud Provider need access and should that employee, during that access, be able to access customer data, he or she must be authorized via the customer's administrators (a

---

42 For example, Microsoft emphasizes the model of shared responsibility or "Division of Responsibility", e.g. https://docs.microsoft.com/de-de/azure/security/security-paas-deployments#division-of-responsibility

43 Top level administrator role: This term is used for conversational purposes. Technically, this term is inaccurate. Rather, it is a result of a segregation of duties where the Cloud Provider manages the underlying Base Components and has nothing to do with the Virtual Machines. The administrator of the Cloud Provider would have means to stop a Virtual Machine, and also could cause a defined Virtual Machines to be launched but would not have access to the Virtual Machine. The ability to stop a Virtual Machines is due to situations of urgency: If a Virtual Machine suddenly has an abnormal state possibly impacting the stability of other Virtual Machines running on the same environment then the Virtual Machines must be stopped.

44 Again, this terminology is technically not accurate (and knowingly, we still use this way of describing the facts for the purposes of simplifying the factual description). Technically, the more appropriate keyword would be segregation. The Bank's administrators could be referred to as VM admins or IaaS admins.

process that is ensured by means of technical and organizational measures). In the overall system, the customer's administrator is the second-highest level administrator.

- The Cloud Provider employee designated as a support manager is given the role of a lower-level administrator for the dedicated period of time for which the customer (the Bank) grants such rights. The eligible administrator can be said to exercise only third-level admin rights.

76 Of course, the above by no means is a complete description of an IaaS model. The explanations serve the purpose of exemplifying interdependencies that foster anonymity. A setup fostering anonymity results in an inherent protection of the customer's Virtual Machines. Of course, many other layers of protection exist. The above explanations are given by way of example and are intended to show that the service model may need to be analyzed and understood in quite some detail, as the service model determines what measures apply and how they interact and overlap.

77 The measures are mostly technical and organizational in nature. Due to the combination of the measures, the likelihood and even the possibility of employees accessing a customer's data on the customer's Virtual Machines is reasonably excluded. The high degree of automation and anonymity inherent in the hyperscale approach thus provides the Bank, as a customer, with a natural protection against unauthorized Plaintext Access by individual employees of the Cloud Provider. The above examples are intended to explain that the setup of the Cloud Provider can actually lead to effective protection of bank customer data.

78 If the Cloud Provider is able to plausibly document such a combination of measures, the Bank can prove that its choice (e.g. "pure IaaS model"), in combination with the documented measures, leads to viable protection against unauthorized access. Then, the Bank will be able to affirm that Plaintext Access by unauthorized personnel of the Cloud Provider will not take place during Normal Operation.

79 The fact that the Cloud Provider provides the "top-level administrators" shows that the Cloud Provider, in theory, would have the ability to access some aspects of the data layer[45], of course, one should add. However, such ability must be understood to be of theoretical nature for as long as the Cloud Provider abides by the rules that apply between the Bank and the Cloud Provider, and for as long as technical and organizational measures have been put in place to ensure that such access does not take place (during Normal Operation). If this can be documented, the Bank can confirm that it is in compliance with the most recent case law of the Swiss Federal Court (according to which only *actual access* counts).

80 Therefore, an IaaS model that has been properly set up can be used by the Bank without breaching Art. 47 Banking Act.

---

45 This statement should be clarified: With a Virtual Machine the data is stored in a VHDX format, which is still protected with the customer's admin password, so theoretically the Cloud Provider could copy the VHDX file and try to hack the admin password offline to be able to access data in the VHDX, but there is never Plaintext Access. In other words, in an IaaS context there are significant restrictions that are dictated by technology.

b) Pure PaaS Offerings

81 A PaaS offering differs from an IaaS offering in that the customer does not manage the Virtual Machines on its own. The Cloud Provider takes over management of the Virtual Machines, including the operating system and the platform software such as database software and the like. All of these components are also completely operated by the Cloud Provider. The Base Components used for the PaaS model are no different from those used in the IaaS model. The way of presenting the benefits of this to the customer is set up differently, however:

- With an IaaS model, a client "books" resources from within its Tenant. As a result, within the identity and authorization system established in the cloud solution, these resources are registered for the customer in a dedicated manner (using logical definitions in the identity and authorization system and in the network system). As already described, from an overall perspective, the Cloud Provider hosts the top-level administrators and the customer the second-highest level administrators.

- With a PaaS model, a service is first set up by the Cloud Provider (the Cloud Provider aggregates a number of services as “standard products”). Thus, in a PaaS context, the Cloud Provider not only hosts the top-level administrators (as must be the case for each cloud solution) but also the second-highest level administrators. If the customer books such standard products from within its Tenant, the identity and authorization system, along with other components relying on logical methods, ensures that the data storage involved in the standard product is connected only to the customer in a unique manner (and not to any other customer). In fact, the customer’s administrators effectively become third-highest level administrator. If the customer requested Tenant-related, dedicated support from the Cloud Provider, the customer's administrator would unlock the support worker (personnel of the Cloud Provider) to grant access to the Tenant – that Cloud Provider’s personnel would then be an “eligible admin” on a level further below.

82 From a technical perspective, the core approach for how the customer retains control over its data in a PaaS environment is Tenant isolation (or “Tenant-level isolation”).

83 In a PaaS environment, as opposed to a mere IaaS environment, the level of organizational measures that are used to protect the customer’s data increase, while technical measures are applied less frequently. That is not at all an issue per se. The relevant question, from a criminal law perspective, is whether a relevant disclosure of protected information takes place, or why which measures prevent such disclosure. It is not relevant whether these measures are technical or organizational in nature. Thus, with a PaaS model, the result does not change (as compared to the IaaS model) – as long as adequate methods for preventing unauthorized access are in place and effective. Thus, the conclusion according to para. 79 et seq. can be carried over to the PaaS model.

c) SaaS Offerings without Foreign Reference (or SaaS Components Added to IaaS or PaaS Offerings)

84 With an SaaS model, the control over the overall system shifts even further towards the Cloud Provider. While the IaaS model still uses a variety of protective mechanisms that are inherent to the architectural DNA of a cloud solution, such technical measures of protection are significantly

less relevant with an SaaS model. In other words, organizational protective measures are even more important with the SaaS model. We do not need to describe these protective mechanisms in detail in this document – the protection available with an SaaS model will always very much depend on the concrete protective mechanisms that have been put in place. It is crucial that the Bank, after analyzing these mechanisms, confirms that, in its best judgment, access by the Cloud Provider's employees to customer data appears very unlikely during the Normal Operation.

3. Conclusion

85 The architectures of mature Cloud Offerings, which are strongly oriented towards the anonymized management of its Base Components, permit the use of external IT Infrastructures without Plaintext-Access (disclosures) during Normal Operation. By ensuring that appropriate technical and organizational measures are taken against disclosures, the Bank can use such Cloud Offerings without violating Art. 47 Banking Law - even without the appointment of the Cloud Provider as its Agent. Such Cloud Offerings are extensions of the physical and logical perimeter of the Bank (see para. 5), but there is no expansion of the personal perimeter.

II. Fallback: Preventing Purely "Incidental Access"

86 Below we discuss the question of whether a support employee of the Cloud Provider may receive Plaintext Access to protected information in individual support situations if the Could Provider has not been appointed as an Agent (otherwise support access would, a priori, be privileged). Such case-based access to protected information may occur in the following situations:

a. Incident: The Bank has a problem *in* its tenant, for the resolution of which it would like to involve one of the Cloud Provider's employees.

b. Maintenance: The Bank is informed that the manufacturer of certain software components is conducting software maintenance work in its Tenant. It would like to use an employee of the Cloud Provider for this work.

c. Support: The Bank would like assistance in carrying out software maintenance work, and it wishes to use an employee of the Cloud Provider for this purpose.

87 The likelihood that the Bank will need to involve the Cloud Provider or its employees in these situations is nearly zero, but it may occur on very rare occasions. A legal assessment of the use of the Cloud Provider by a Bank is provided below. However, it must be noted that such scenarios are very rare.

88 The "Cloud" per se does not exist (para. 67 et seq.). This is clearly demonstrated by the foregoing statements. We will not make further distinctions based on service model here. Instead, we will focus solely on a comparison of an IaaS solution and an SaaS solution.

1. IaaS Model

89 If an employee of the Cloud Provider receives remote access to, for example, the Bank's virtual machine (because the Bank grants such access) and in this context the employee gains Plaintext Access, the Bank must monitor the employee's movements in the Virtual Machine. The Bank may

only grant control of the screen to the Cloud Provider's employee in exceptional cases (only when necessary – "need-to-know" basis). It is generally not necessary for the Cloud Provider employee to exercise such control him or herself. Instead, the Bank employee can exercise the control him or herself by issuing verbal instructions to the support employee. However, if, as an exception, it is necessary for the Cloud Provider employee to briefly assume control of one of the Bank's virtual machines, the Bank employee must all times be able to stop or pause the processes. In this case, the Bank employee may not leave the screen at any point.

90 Furthermore, in terms of support there are a limited number of conceivable situations in which the Cloud Provider employee would need to view the customer data. There is only said to be a disclosure if this is the case. Disclosures are generally not permitted. Accordingly, the Bank must generally refrain from making such support requests.

91 Where such support requests that result in the disclosure of bank customer data are necessary, the Bank is generally able to develop a mitigating mechanism or devise a workaround.

92 Potential workarounds include the following:

a. The Bank involves a local Agent, formally appointing him/her as an Agent and having him/her carry out this special task (possibly with offline support by the Cloud Provider).

b. The Bank anonymizes bank customer data or temporarily deletes it from the system.

c. The Bank temporarily creates an identical digital copy of the Virtual Machine without the customer data and presents a visual representation of the problem to the Cloud Provider's support employee on this basis.

93 Mitigating mechanisms may include combinations of measures. If a support employee of the Cloud Provider does need to be granted access, the support employee may be integrated in the Bank's control authority on the basis of very strict confidentiality rules (e.g. with substantial contractual penalties). Consequently, the support employee formally becomes an Agent for this specific activity. Otherwise, a solution that leads to effective control by the Bank must be found for the individual situation.

94 Finally, scenarios are conceivable that would provide justification in individual situations, such as emergencies or petty lawsuits. Such scenarios should, however, be considered and assessed cautiously as part of a preliminary risk analysis. Such scenarios are justified only if they are absolute exceptions. If they were regularly occurring events, they would have to be considered part of Normal Operation, which would result in a different assessment of them.

95 In summary, there are, even for the (very rare) scenarios described above in which there is incidental access, numerous arrangements with an IaaS model that do not involve disclosure or the opportunity for presenting justification. As a result, support does not a priori represent a general and comprehensive prohibition against the use of Cloud Offerings.

2. SaaS Model

96 With SaaS components a distinction based on Virtual Machines usually can no longer be made, as such Virtual Machines are generally not assigned to an individual customer. The analysis here is based solely on *Tenants*, i.e. logically separate access areas that are provided to the customer via multiple Virtual Machines. Here, too, a distinction based on whether the Cloud Provider must carry out the work specified in para. 80 within the Tenant or outside of the Tenant.

97 With the SaaS model, the Cloud Provider is much "closer" to the Tenant used by the customer than is the case with the IaaS or PaaS models. The software architectures are also set up differently and often separate the resources used only by the customer less precisely than those managed entirely by the Cloud Provider.

98 At any rate, the Bank's options for storing information about its customers in the Cloud Provider's IT architectures in a manner that a priori prevents the Cloud Provider from gaining knowledge of it depend heavily on the solution design that the Cloud Provider has established. Only if the Cloud Provider has made architectural arrangements to ensure that the Tenants set up in the SaaS model are separate from the Base Components required for application management and software maintenance can the Cloud Provider, based on this arrangement, implement clear organizational rules for preventing its employees from accessing the customer's Tenant. The selection of SaaS models therefore requires even greater care on the part of the customer. The requirements imposed on the internal department at the Bank that is responsible for procurement increase with these models. However, if the Cloud Provider has arranged for such IT architectures, it may also offer the customer processes that proactively reduce and largely avoid contact points with the customer's Tenant.

> *Individual Cloud Providers have, for example, established special protective measures of an organizational nature for work involving the risk that the customer's Tenant will be accessed. These include such measures as a process model called a "customer lockbox" (a purely organizational measure) from Microsoft. With this system, a support employee can, on the basis of internal directives, only access the relevant Tenant if he or she has completed certain procedures. Microsoft states in its marketing documents that it has rarely ever been necessary for Microsoft to have to access the Tenant or the data stored in the Tenant (exceptions, of which the customer is proactively informed and to which it may grants its consent in advance, are exceedingly rare).*

99 If the IT architecture does not include the basis for such organizational measures, many Cloud Providers establish a mechanism by which access logs review the extent to which an employee may access a Tenant without a need to know.[46] This protection has a proactive effect because employees know that they will be checked to determine if they have accessed information without permission and, in the event of a breach, they will be subject to stringent sanctions. Otherwise, however, logs only enable retroactive control of the Cloud Provider's conduct.

---

46 These access logs are of immense importance if the Cloud Provider allows auditing. Audits are conducted according to internationally recognized standards (e.g. International Standard on Assurance Commitments, ISAE, managed by the International Federation of Accountants, IFAC), distinguishing standards on the reliability of financial information (ISAE 3402) from standards concerning the integrity and protection of other information (ISAE 3000) (similar to the distinction SOC 1 v. SOC 2, where "SOC" stands for "Service Organization's Controls"). During such audits, certain access logs are often fully validated, allowing at least some subsequent control over the reliability of the Cloud Provider's actions. A distinction is made between pure one-time surveys (type I, type 1 or in other standards also type A, "snapshots") and surveys extended over a longer period of mostly half a year (type II, type 2 or other in other standards also type B).

100 Conclusion: There are technical setups and organizational mechanisms that can prevent a disclosure for operational activities to a sufficient extent, even with SaaS models.

3. Findings

101 The foregoing considerations show that for such support as may be requested either the Bank will not work with the Cloud Provider (maintenance work with the IaaS and PaaS models for the Bank's own applications) or that various security mechanisms can be established in order to protect the integrity interests of the Bank and its bank customers during Normal Operation.

102 In the context of maintenance work, incident handling and support requests, there is no a priori prohibition against the Bank using Cloud Offerings from trustworthy and carefully audited Cloud Providers that have been set up in line with state-of-the-art technology.

CONCLUSION: SWISS BANKS CAN USE MATURE CLOUD OFFERINGS

On the whole, considerations related to the contractual relationship between the Bank and bank customer (para. 7 et seq., para. 10 and para. 12), general criminal law doctrine (para. Art. 11 CC, see para. 21 et seq., and, in particular, para. 25, and Art. 12 CC, see para. 27), constitutional considerations (para. 11), the latest case law (para. 16) and nearly unanimous opinion at present lead to the same conclusion: A Bank must be allowed to use IT Infrastructures if these IT Infrastructures are protected with adequate measures (for the state-of-the-art technology, see para. 25). The focus here is not on who operates these IT Infrastructures.

Thus, this legal opinion shows that Swiss Banks may use Cloud Offerings if they select a reliable Cloud Provider with a mature IT Infrastructure in the framework of a careful procurement process. Technical, organizational and, to some extent, contractual measures can provide such Cloud Providers with adequate protection for confidential information.

As long as the Cloud Provider ensures that the information and the underlying data that the Bank has migrated to the Cloud Provider's IT Infrastructure is nowhere and at no time accessed in an unauthorized manner, the Bank will not be in breach of the objective elements of Art. 47 Banking Act – even if it does not appoint the Cloud Provider as an Agent.

Cloud Providers may be appointed as Agents of the Bank. In practice, however, the significance of the integration of the Cloud Provider as an Agent within the meaning of Art. 47 Banking Act cannot be overstated. If the Bank tracks in detail how difficult processes are implemented at the Cloud Provider, in most cases it will find that there are no significant disclosures – which makes integration of the Cloud Provider as an "Agent" in and of itself unnecessary. However, such assurance is required on the basis of Art. 11 para. 2 CC and Art. 12 para. CC, even if the Bank appoints the Cloud Provider as an Agent.

* * *

APPENDIX: DEFINITIONS OF TERMS USED IN THIS LEGAL OPINION

In this Legal Opinion, the following terms are defined as follows:

Cloud Provider is the entity providing IT services based on Cloud Computing.

Foreign Cloud Offering / Provider are references to either the Cloud Provider (legal domicile, etc.) or the Cloud Offering (data center location, location of employees or involved third parties, etc.) with a foreign connection. A foreign connection means, for example, if (i) a Cloud Provider has its legal domicile abroad; (ii) a Cloud Provider operates IT Infrastructures abroad; or (iii) the Cloud Provider's employees or subcontractors are abroad.[47]

Bank is each entity subject to the Banking Act pursuant to Art. 1a, Art. 1b and Art. 2 Banking Act.

Base Components is a term used to express where the Cloud Provider's operating services are targeted. The term Base Components describes the IT Infrastructures as such, but not what can be performed or displayed by them (the Tenant, as a logical representation of certain functionality enabled by means of the Base Components). Rather, Base Components means the basic metal machines plus applications deployed on them. Base Components are managed in the background.

Cloud Offering, or **Cloud Solution**, is the set of services that a Cloud Provider makes available to customers, such as Banks, to permit the use of certain IT Infrastructures, in a standardized, automated, scalable manner, over data networks, but not necessarily dedicated to only one customer. Cloud Offerings can permit the Bank to downsize or even abandon some of its own data centers, own hardware and own server software (in the context of Infrastructure as a Service, IaaS) or serve to ensure that the Bank does not need to operate certain software itself (operating software or user applications; when using Platform as a Service, PaaS, or Software as a Service, SaaS). In the present memorandum, Cloud Offerings, as a term, refers to "public cloud", a term that has been colloquially coined in order to express that the Base Components of the IT Infrastructures in use by the Cloud Provider are not made available in an individually exclusive manner ("dedicated") to each customer. (However, the functionality offered to the customer as part of the Cloud Offering (see Tenant) is customer-specific and isolated from what other customers see; isolation is made possible by means of modern network technology.)

IT Infrastructures refers to the totality of buildings, hardware, software, network technology, etc. that a Cloud Provider uses to provide a Cloud Offering.

Plaintext Access refers to the process by which a person can easily recognize, read and remember or pass on the meaning of the signs discernible by him. In contrast, mere access to the location of the data storage does not constitute Plaintext Access. Anyone who is allowed to visit a server room and strolls past the data carriers in the corridor between the servers obviously has access to data (more precisely, to the location of the data storage). Even if he or she does so without supervision, he or she does not,

---

[47] For this category (employees or subcontractors), the foreign reference valid when then Clod Offering can be accesses from abroad.

merely by walking by, see the contents stored on the media[48]. If the visitor subsequently leaves the server room without accessing the data carriers, nothing has happened in relation to the secret to be kept. Similarly, we do not speak of Plaintext Access if someone needs a technical tool before he or she can discern what is stored on the media. Such a tool could be a screen attached to a data processing device or an application that accesses a database and (only) by means of which the information stored in the database becomes transparent to the user. The term is important for an understanding of secrecy obligations. However, Swiss law does not provide any suitable terminology for distinguishing information that is recognizable to humans from technically formatted signs that can only be interpreted by machines (but that cannot be recognized by people without an additional instrument). Accordingly, we use this colloquial term in this Legal Opinion.

Normal Operation[49] means that the Cloud Offering is operated by the Cloud Provider as planned (as opposed to exceptional situations that are not Normal Operation, such as: Bankruptcy[50] of the Cloud Provider, access by a public authority[51] to the Base Components, unlawful access by criminals to the Cloud Solution).

Tenant is the customer-specific environment provided by the Cloud Provider to the customer. It is an area that is only available to the customer and its employees (isolation). Network technology is used to enforce such isolation. A Tenant usually is provided by means of a variety of Base Components. It is worth noting that it is often not possible to exactly identify what specific Base Components are used to set up a Tenant for a customer.

Virtual Machine is an emulation of a computer system. Such emulation is enabled through the Base Components. Thanks to a number of Virtual Machines, the Cloud Provider is in a position to offer Tenants to customers.

---

48 Therefore, we sometimes use the term Content Layer instead of the term Plaintext Access. From the perspective of this legal memorandum, the term Code Layer is used to some extent as the opposite to the term Content Layer. We use the term Code Layer to refer to signs that are only machine-readable, which means that someone who wants to read or see the Content Layer needs additional instruments (such as an application plus some hardware running on it, a screen, etc.) to read the Content Layer. The point is that the Content Layer is not visible to an outsider only because formatted data (even if not encrypted) is loaded on an IT Infrastructure he or she controls. Only after taking additional steps would this be the case.

49 This distinction is based on the fact that a Bank is only required to take account of the legal risks of a disclosure to the extent that it can control such risks. However, if certain risks can be anticipated in the abstract, they may trigger information obligations to bank customers.

50 The Bank must plan for this scenario carefully and must also monitor the Cloud Provider with respect to the risk of bankruptcy. This includes the obligation on the part of the Bank to maintain close interaction with the Cloud Provider's key account manager and to review the Cloud Provider's financial statements on a regular basis. The Bank must also be able to measure its business continuity planning in terms of such scenarios (in order to enable quick backsourcing and the careful deletion of data). For example, it must have a contingency plan according to which the Bank is able to quickly and directly delete confidential data via the customer portal's control panel as soon as the Bank learns of the Cloud Provider's bankruptcy – and it must be able to do so before the appointed liquidator blocks the Bank's access to the Cloud Provider's IT Infrastructure.

51 For example, a law enforcement agency asks the Bank or the Cloud Provider for access to the data of a bank customer (or the Bank's data). Very few authors properly discuss the risk of access as a result of foreign criminal proceedings, i.e. without devolving into an often fuzzy discussion of such topics as the CLOUD Act, the US PATRIOT Act and similar provisions of foreign criminal law. The risk of access by domestic authorities that cannot be described as Normal Operation must also be discussed. Access by a Swiss authority can have similar or even more dramatic effects than access by a foreign law enforcement agency. Of course, the reverse is true, too. The Bank generally does not know what the bank customer's risk exposure is in this respect. However, the Bank must understand the likelihood and the circumstances under which a government agency may access its data (irrespective of its use of Cloud Offerings).