walderwyss attorneys at law

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Telephone +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

Legal Opinion

prepared for Swiss Bankers Association (SBA)

by Walder Wyss AG (Dr. Michael Isler, Oliver M. Kunz. Dr. Thomas Müller, Dr. Jürg Schneider, Dr. David Vasella)

concerning **Permissibility of disclosure by Swiss banks of bank client information to agents in foreign countries under article 47 of the Banking Act (BA)**

Date 15 February 2019 / 9101398v1

[*Convenience translation dated 25 March 2019*]

Contents

1. Background

1 The Swiss Bankers Association (**SBA**) has requested that we prepare the present opinion in order to answer the following question:

> *Is a Swiss bank in breach of the bank customer confidentiality under article 47 para. 1 and 2 of the Federal Banking Act (**BA**) if it transfers customer identifying data as part of a processing arrangement?*

2 The statements in the present opinion are limited to answering this question. In particular, the following subject areas are not the subject of this opinion:

(a) The material scope of application of article 47 BA.

(b) The Federal Data Protection Act (**FDPA**);

(c) Confidentiality provisions outside of those in article 47 para. 1 and 2 BA, such as article 273 of the Swiss Criminal Code (**CC**) and article 35 FDPA; and

(d) Foreign law.

3 The question addressed is to be understood against the background of a preliminary draft V2.5 f SBA's „*Cloud Leitfaden – Wegweiser für sicheres Cloud Banking"* (the **Guidelines**). We refer in this opinion to the illustration in the Guidelines, but we do not comment on the completeness or adequacy of the technical and organisational measures referred to in the Guidelines or on the question of what combination of measures is appropriate in a specific case. Thus, the Guidelines make no claim to completeness and stipulate that, in using the Guidelines, Banks should take into consideration their size and the complexity of their risk model on the basis of risk and proportionality.

4 In this opinion we speak from time to time of „outsourcing" and „involvement of a service provider" and in doing so we mean that a bank makes use of the services of an IT provider – such as a cloud provider – and that in this connexion the provider has or may have access to information subject to bank client confidentiality. In this context, we go into technical issues such as various service models in only a very limited way.

2. Conclusions

5 We are of the opinion that the involvement of service providers by a bank and the disclosure of CID (customer Identifying data) to the service provider is permissible:

(a) So long as the involvement is in accordance with a reasonable interest of the outsourcing bank, the service provider supports the bank's business activities and is subject to its authority to issue instructions and the bank itself provides the services agreed to with the bank's client; and

(b) if there is no express or tacit agreement with the bank's client that the involvement in question is impermissible.

6 This stems primarily from article 68 of the Swiss Code of Obligations (**CO**). There is no evident basis for restricting this principle to domestic matters. The principle therefore also applies if a bank outsources the processing of CID to a service provider abroad or if the foreign service provider gains access to CID in connexion with its activities for the bank. Accordingly, we are of the opinion that, from a civil law perspective, a bank may also outsource CID to a foreign service provider, e.g. within the framework of a cloud solution, even if in doing so the service provider gains or can gain knowledge of the CID.

7 Bank client confidentiality (article 47 para. 1 and 2 of the Banking Act, **BA**) is to be understood as a reinforcement through criminal law of confidentiality obligations based on civil law. Therefore, if outsourcing by a bank is permissible under contract law, it is also permissible under criminal law, which is why the above-mentioned principles also apply here. The involvement of a service provider and the disclosure of CID to it is therefore also permissible in principle under article 47 para. BA even if the service provider is located abroad. If, on the other hand, a contractual agreement between the bank and the bank's client provides for a prohibition on the outsourcing of CID as covered by bank client confidentiality, compliance with that agreement is also subject to criminal law under article 47 para. 1 and 2 BA.

8 The question posed at the beginning must therefore be answered as follows:

> *A Swiss bank is not in breach of the Bank client confidentiality under article 47 para. 1 and 2 of the Banking Act (BA) if it transmits CID to a recipient abroad in the context of an outsourcing, provided that*

> *(a) the outsourcing is in a reasonable interest of the bank, the auxiliary assists the business of the bank and is subject to ist power to give directions and the bank provides the services agreed with the bank customer substantially on its own account; and*
>
> *(b) there is no explicit or tacit agreement with the bank customer that indicates that the outsourcing in question is not permitted.*

9 Consequently, the disclosure of CID in the context of such outsourcing does not constitute an inadmissible disclosure within the meaning of article 47 para. 1 BA even if the service provider is located abroad and is able to gain access to the data in connexion with its activities.

10 Only if an *unauthorised* third party becomes aware of CID is there a disclosure that could be an offence within the meaning of article 47 para. 1 BA. However, such a disclosure is only subject to Swiss law if it takes place in Switzerland. In addition, article 47 BA does not provide for strict liability, but only comes into play if the bank acts intentionally or negligently, i.e. if it fails to take the necessary security measures and thereby causes (or contributes to causing) the disclosure. For this reason, the bank, whenever outsourcing, must exercise the due care required by the circumstances in order not to expose itself to the charge of negligence, including under the criminal law.

11 In this context, of course, the Bank does not have to rule out any possibility of disclosure. Only the creation of an *unlawful* risk is negligent. For this reason, there is no negligence if the bank has exercised the care required by the circumstances. In this regard, the required care must be substantiated first and foremost by the applicable data protection law, by the requirements of FINMA circular 2008/21 (Operational Risks Banks) (**Circular Operational Risks**) (Annex 3) and by the Federal Data Protection and Information Commission (**FDPIC**)'s guide for technical and organisational measures for data protection. Other technical standards must also be included as applicable, insofar as they represent the state of the art. In addition, compliance with the required care necessitates an assessment of the risks to the bank's client resulting from the outsourcing. In this connexion, the bank must assess general and provider-specific risks associated with outsourcing, along with the specific foreign risks, if any. In this context, the facts that may play a role include the location where CID is or may be stored and from which access is possible; the legal risks to the provider in the event of an infringement under applicable local law; the legal and factual

possibilities of access by local authorities at the relevant locations and the resulting risks to the bank's clients; and the potential, if any, of access by authorities located outside the location of the data that may be triggered by the outsourcing (such as those due to the US CLOUD Act[1]).

12 In summary, it can be seen that the outsourcing bank can be held accountable in the event of disclosure to an unauthorized third party only if it did not exercise the necessary care in the outsourcing and this was the cause of an unauthorized disclosure. The fact that outsourcing (in particular abroad) or granting the possibility of access to a service provider increases in the abstract the risk of unauthorised access is not in itself sufficient to establish negligence on the part of the bank.

3. Basic Principles

13 Article 47 BA reads as follows:

[*see original*]

3.1. Aim of the protection of bank client confidentiality

14 In the further course of this opinion, the legal basis of bank client confidentiality plays a role. In this regard, two different approaches stand out:

(a) Bank client confidentiality safeguards the bank's non-disclosure obligation to its clients under criminal law, which is based on civil law (protection of the individual);

(b) Bank client confidentiality serves primarily the public interest in a functioning financial market, with the protection of bank client data as an essential pillar (protection of the system or function).

15 This distinction has an impact on the freedom of action of the bank with regard to bank client confidentiality and the significance of the customer's level of expectation. Whereas a bank can on the one approach condition the acceptance of business relationships basically on the client's waiver of bank client confiden-

[1] [*see original*]

tiality, on the other approach limits to its freedom of contract are set by the public interest. The risk assessment is also different in the context of outsourcing. In the case of individual protection, the client's expectations regarding the bank's business practices and the negative effects on the client of a breach of confidentiality are paramount, while in the case of protection of the system the negative effects on the Swiss financial market must be considered first and foremost.

16 Conceptually, the prevailing view assumes that bank client confidentiality safeguards the obligation to maintain professional secrecy under the civil law – i.e. contractually and as a personal right.[2] In this respect, article 47 para. 1 and 2 BA has no further substantive scope of application than the privacy obligations under article 398 para. 1 in conjunction with article 321a para. 4 CO and under article 28 of the Swiss Civil Code (**SCC**).

17 As we see it, this view is correct. It is supported by the 1970 dispatch regarding the revision of the BA:[3]

[*see original*]

18 The dispatch regarding the banking initiative of 1982 leads in the same direction – but somewhat less clearly.[4] In 2012, the Federal Council also stated clearly that bank client confidentiality is based on civil law:[5]

[*see original*]

19 However, the legislative materials also contain statements that can be read as references to system protection, as in the dispatch of 1934 regarding the issuance of the BA:[6]

[*see original*]

20 Later, in connexion with a strengthening of article 47 BA prompted by the FDP.Die Liberalen that came into force on 1 July 2015 with the federal law of 12 December 2014 on the expansion of criminal liability for the violation of profes-

[2] [*see original*]
[3] [*see original*]
[4] [*see original*]
[5] [*see original*]
[6] [*see original*]

sional secrecy, the reference was clearly to the public interest. In its comment of 13 August 2014 on the report of the relevant commission, the Federal Council stated:[7]

[*see original*]

21 Thus far, the Federal Court has not expressed itself clearly on the issue. However, there are statements that can be understood as an indication of system protection. Thus, the Federal Court held in decision 141 IV 155 E. 4.2.5 (although with reference to the protection of the Bank's professional secrets and therefore a topic outside the scope of bank client confidentiality):

[*see original*]

22 In several subsequent decisions with reference to international judicial assistance[8], the Federal Court has held that important interests of Switzerland in the matter of former article 1 para. 2 and present-day article 1a of the Mutual Assistance Act (IMAC) may be affected:

[*see original*]

23 In connexion with article 273 CC, in 1985, the Federal Court also emphasised the system relevance of trust in the bank:[9]

[*see original*]

24 On the other hand, the Federal Administrative Court in a 2010 decision clearly understood that bank client confidentiality was bound to individual protection:[10]

[*see original*]

25 Following the dispatch of 1934 and the case law referred to above, the literature also contains the view that article 47 BA also protects the financial mar-

7 [*see original*]
8 [*see original*]
9 [*see original*]
10 [*see original*]

ket.[11] Finally, Kurz/Zollinger reflected this view.[12] In this regard, they argue that in certain respects article 47 BA is stricter than article 321 CC. Violation of article 47 BA represents a public offence and is also punishable in the case of negligence, while dissemination and attempted dissemination are also punishable.

26 In our opinion the argument that bank client confidentiality also serves the purpose of functional protection is not so weighty that it would cause the prevailing view to be set aside. In particular, the stronger protection in comparison to article 321 CC does not support the conclusion that the aim of article 47 is functional protection:

(a) The fact that article 47 BA is established as a public offence can be explained by the fact that foreign bank customers could not possibly observe the short application deadline.[13] Thus, the increased protection is in general warranted by the fact that specific risks, such as trade in stolen data, would be encountered in the area of bank client confidentiality (once again based on private law).

(b) Privacy also receives increased protection under criminal law in other areas, such as the European General Data Protection Regulation, and, according to the Federal Council's will also in the future FDPA, and here again the argument is not functional protection, but the increased threat to privacy and the need for deterrence.

27 It is also not sufficiently clear from the cited case law that the purpose of bank client confidentiality is functional protection. It is true of course that an erosion of bank client confidentiality could damage the economy (see para. 21 above). However, this does not permit us to conclude that bank client confidentiality provides functional protection. Although there is obviously a public interest in Swiss legal institutions not being undermined, this says nothing about the protective purpose of a threatened legal institution. The decisions regarding international judicial assistance are also to be understood in the same light (see para. 22 above). Here again, this may relate more to the basic interest in institutional protection and less to bank client confidentiality itself serving a protection purpose. Finally, the increased range of penalties under article 47 BA through the creation of the Financial Market Supervision Act (**FINMASA**) is in-

[11] [*see original*]
[12] [*see original*]
[13] [*see original*]

dicative of functional protection. In fact, the increased sentences definitely relate to protection of the system and of creditors and investors.[14] However, the increase in the range of penalties under article 47 BA was probably owed to standardisation.[15] It cannot be denied that individual protection always serves the purposes of system protection. In this connexion, however, it is noteworthy that all the comments that attribute a system character to bank client confidentiality have in mind a *large-scale* violation of bank client confidentiality. This viewpoint is consistent with the fact that the banks' duties of care and supervision under principle 9 of annex 3 of Circular Operational Risks regarding outsourcing services and major contracts related to CID are considered *mandatory* for all types of activities that involve access to *mass CID*.[16] However, bank client confidentiality does not intend to sanction only large-scale breaches of confidentiality, but also each individual case. Consequently, as before, we therefore consider the prevailing view the correct one.

3.2. The concept of confidentiality in article 47 BA

28 Article 47 BA does not recognise any independent concept of confidentiality, but is based essentially – but with limitations (see below) – on the accepted understanding of confidentiality in criminal law.[17] There confidentiality requires all of the following elements:[18]

(a) *Not publicly known*: Only relatively unknown information can be a secret, i.e. information that is neither well-known nor generally accessible;

(b) *Intent to keep secret*: The owner of the secret has the intent to limit knowledge of the secret fact to a certain circle of persons. In addition, the intent to keep the knowledge secret must be discernible, and this may also result from the circumstances; and

(c) *Interest in secrecy*: Keeping the fact secret is an interest of the owner of the secret that is worth protecting, based on objective criteria.

---

14 [*see original*]
15 [*see original*]
16 FINMA circular 2008/21, annex 3, para. 47. Here „mass CID" is to be understood as a quantity of CID that is significant in comparison to the overall number of accounts or total size of the private client portfolio.
17 [*see original*]
18 [*see original*]

29 However, the third element under article 47 BA does not apply without limitation. Since the criminal liability for bank client confidentiality is based on private law (see para. 14 et. seq. above) and the purpose of private law is not objective secrecy, but rather confidentiality in general,[19] what is objectively worth keeping secret cannot be of critical importance. Therefore, only the client's interest in maintaining secrecy is significant if, as an exception, the claim to secrecy is not legally abusive.[20]

30 Anonymous information, i.e. information not attributable to a natural or legal person, is not protected by article 47 BA.[21] In this connexion, under Swiss law one must fall back on the criteria of data protection law for reference to the individual. Thus, bank client data are all details that refer to a specified or specifiable person (article 3 item a FDPA), the Federal Court describes the specificity criterion as follows:[22]

[*see original*]

31 Therefore, information is anonymous when, taking into consideration all circumstances, and in particular the technical capabilities and the interest in learning of the information subject to bank client confidentiality, the possibility of revelation is not be expected on the basis of common everyday experience.[23] Accordingly, no disclosure of CID is present in any case if the revelation of CID is impossible, such as when the information in question is anonymised or pseudo-anonymised or encrypted in such a way that the recipient cannot make a personal identification (see para. 41 of the Guideline; cf. also Circular Operational Risks, annex 3, para. 65).

3.3. The notion of disclosure

32 Article 47 BA para. 1 prohibits the „disclosure" of an entrusted or perceived secret. At the same time, the term of disclosure is not defined. It is be deduced from a general term of disclosure found in criminal law. In this regard, disclosure always refers to an unauthorised third person, i.e. a person different from the owner of the secret and from the holder of the secret or their employees

[19] [*see original*]
[20] [*see original*]
[21] [*see original*]
[22] [*see original*]
[23] [*see original*]

and service providers[24] (with reference to service providers see para. 47 et. seq.), which is readily derived from the wording of article 47 para. 1 item a BA.

33 Under previous case law,[25] merely making it possible for a third person to acquire knowledge of the information and not simply its actual revelation is considered to be disclosure. In decision 6B_1403/2017, however, the Federal Court expressly moved away from this interpretation, finding that actual knowledge by third persons is necessary:[26]

[see original]

34 If one also follows this case law for article 47 para. 1 and 2 BA, careless storage of data, for example, would not be sufficient for disclosure to occur so long as the lack of care does not lead to actual knowledge of the data by an unauthorised person. Schwarzenegger, Thouvenin, Stiller and George also come to this conclusion on the basis of their opinion on the use of cloud services by attorneys.[27] Following the above decision, they hold further that this concerns an offence defined by the result rather than by the activity.

35 The preponderance of the earlier literature is of the view that the possibility of revelation is already enough.[28] Earlier jurisprudence was also along the same lines, as for example the Zurich Superior Court in a 2017 decision:[29]

36 [*see original*]

37 The Federal Criminal Court found likewise, last in 2013.[30]

38 However, these decisions and doctrinal views are of earlier date than the decision of the Federal Court referred to above. In addition, there is no indication that the criminal disclosure conduct is to be understood differently depending on the secret. In fact, a uniform definition of disclosure is to be assumed. Therefore, disclosure in the sense of article 47 para. 1 and 2 BA is consummated only through the discovery of the secret by an unauthorised third person.

---

24 [*see original*]
25 [*see original*]
26 [*see original*]
27 [*see original*]
28 [*see original*]
29 [*see original*]
30 [see original]

Hence, in the case of a (contingent) intentional release with no revelation, at most a criminal attempt under article 22 in conjunction with article 333 CC would be involved (see para. 39 f.).[31]

39 It follows as a preliminary result that:

(a) The authorised revelation of CID (e.g. to a service provider acting under an authorised contract) does not represent a punishable disclosure, even if the service provider is located abroad;

(b) The revelation of CID also does not represent a punishable disclosure if the data in question does not reliably represent a reference to individual persons for the recipient, i.e. when it is anonymised or pseudo-anonymised so that it cannot be attributed by the recipient to any person;

(c) Finally, the revelation of CID does not represent a punishable disclosure if it does not lead to an unauthorised third person actually having knowledge of the CID in question. This can also apply even in the case of careless storage of CID if the carelessness remains without consequence. In this case, however, a punishable attempted disclosure may be present with appropriate (contingent) intent.

3.4. Subjective requirements

40 Subjectively, article 47 para. 1 and 2 BA presupposes intent or negligence:

(a) In the case of a crime of intent, the intent must refer to all objective elements of the offence,[32] i.e. including unauthorized knowledge of the CID (see para. 32 et. seq. above).

(b) In the case of negligent violation of banking secrecy, a violation of the duty of care which the bank is required to show depending on the cir-

[31] [*see original*]
[32] [*see original*]

cumstances (article 12 para. 3 CC) must cause the unauthorised disclosure (for specifics cf. para. 65 et. seq. below).

41 Therefore, the revelation of CID does not represent a criminally punishable disclosure where the bank acts neither intentionally or negligently, if it results (nevertheless) in becoming known by an unauthorised person. In this connexion, it must be determined specifically whether any violation of the duty of care is attributable to the bank, since, even in the case of careful storage, it cannot be ruled out that the service provider has committed an error. In particular, it must be determined specifically if the specific duty of care that is violated existed at all (in accordance with the permitted division of roles between the bank and the service provider) existed, since in the first place it is only that person that can have violated the duty of care and therefore acted negligently. In this connexion, the bank's list of duties is limited to the duties related to selection, instruction and supervision that it must observe in accordance with relevant regulations and standards. If the bank has complied with these duties, it cannot be accused of negligent conduct because of the violation of a duty delegated to a service provider.

42 What's more, only the creation of an *unlawful* risk can be grounds for negligence.[33] The fact that an activity (such as the storage of data processing) is associated in general with foreseeable risks to legal interests that cannot be excluded if the required care is exercised must be accepted (unless the legislature has prohibited the corresponding activity *per se*, which is clearly not the present case). Accordingly, it cannot be concluded that the duty of care has been violated simply because a residual risk has arisen.

43 Thus, a criminally liable attempted disclosure is conceivable only in the case of intent,[34] i.e. if the bank intends, or at least at least recklessly accepts, that CID will be become known to an unauthorised person, but this result does not then arise.

3.5. Punishability of the offence in foreign countries

44 Basically, the CC is territorially applicable to acts committed in Switzerland (article 3 para. 1 CC, principle of territoriality), the place of commission under arti-

[33] [*see original*]
[34] [*see original*]

cle 8 para. 1 CC including the place where the harm arose and the place where the harm occurred (principle of ubiquity). The place of commission is initially where the criminally punishable conduct objectively was carried out, thus, in the case of unauthorised disclosure, it occurred where the disclosure took place. Therefore, if a Swiss bank discloses CID without authorisation, the place of commission is Switzerland, while if a service provider located in a foreign country reveals CID without authorisation, the place of commission is the foreign country concerned.

45 The place where the harm arose is therefore the place where the result of the offence comes about.[35] Following the decisions of the Federal Court, according to which the offence of violation of secrecy presumes that the secret becomes known (see para. 32 et. seq.), the result can only be located where this revelation arises, i.e. in the place where the unauthorised recipient of the information is situated when the information is received.

46 Thus, if a bank transmits CID in an authorised manner to a service provider in a foreign country who makes this CID known to a third person in a prohibited way in a foreign country (e.g. to a foreign government agency), the place where the harm arose can only be the foreign country in question. In this situation, neither the place where the harm occurred nor the place where the harm arose is Switzerland with reference to the service provider. Therefore, its punishability depends, among other things, on whether the conditions of article 7 CC are satisfied, i.e. whether the disclosure is also punishable in the foreign place of commission.

47 In this situation, on the other hand, a place of commission in Switzerland is present[36] if the bank infringes the duty of care incumbent on it (see para. 40 above) and by doing so contributes causally to the result, so that in this instance a risk of criminal liability exists.

4. Permissibility of outsourcing CID to a service provider

48 The fact that only disclosure to an *unauthorised* person is liable to prosecution, although not stated explicitly in article 47 para. 1 BA, is self-evident. In this

[35] [*see original*]

[36] It is sufficient that the unlawful acts be performed only partially on Swiss soil. Cf. in this regard decision 6B_86/2009 of 29 October, consideration 2.3.

connexion, the question arises as to whether and under what circumstances a secret may be entrusted to a provider.

4.1. Permissibility of outsourcing to service providers

49 It is unquestionably permissible to outsource CID[37] that is subject to bank client confidentiality if this does not result in its revelation, i.e. if the service provider gains no knowledge of the CID. From a practical perspective, however, this is conceivable only in the case of storage solutions if the service provider received encrypted data and this data cannot be decrypted.

50 With regard to the disclosure of unencrypted CID (or of encrypted CID that the service provider can access in general or under certain conditions), the view is taken, particularly by *Wohlers*, that the outsourcing of CID requires the consent of the bank customers in question.[38] Initially, it may be argued against this view that the involvement of a service provider is in many situations indispensable and also serves the interests of the bank's customers. In the first place then, *Wohlers's* view is not practical. But it also contradicts the position of the Federal Council, which for several decades now has considered the outsourcing of certain services to agents with revelation of CID as permissible. In the 1971 revision of the Banking Act, the bank's „agents" were included among the persons subject to professional secrecy under article 47 para. 1 BA. The 1970 dispatch[39] states in this regard:

[*see original*]

51 This makes clear that the outsourcing of CID to agents, e.g. in the IT area, is essentially permissible according to the intent of the Federal Council. The Federal Ministry of Justice has also taken the position in an unpublished opinion of 21 June 1999 that the outsourcing of invoicing and IT services by physicians without the permission of the patients was also permissible.[40]

52 The case law also assumes that outsourcing by banks is basically permitted. For example, in decision 121 IV 45 (consideration 2a) the Federal Court held:

---

37 Here „outsourcing" is more or less synonymous with „disclosure".
38 [*see original*]
39 [*see* original][40] [*see original*]
40 [*see original*]

[*see original*]

53 In an 2015 decision the Zurich Superior Court stated:[41]

[*see original*]

54 In 2016 the Lucerne Canton Court even stated as follows:[42]

[*see original*]

55 For other professional secrets as well, the case law has considered outsourcing to be permitted. Thus the Zurich District Court held that the involvement of a „secretarial pool" by a physician was permitted since the secretarial pool qualified as a service provider.[43]

56 The literature has also challenged *Wohlers*, insofar as it has addressed the subject.[44]

57 From all of this, it must be concluded that outsourcing must in principle be permissible even if the service provider is able generally or under certain circumstances to gain access to the unencrypted data. In this connexion, the actual need for outsourcing is not required. In each of the cases we assessed, an appropriate practice or an interest in optimising customer relations could suffice. The literature in many cases also assumes that outsourcing without the bank customer's consent is permitted if notice is given.[45] However, in agreement with the case law cited, these writers required that the outsourcing:

---

41 [*see original*]

42 [*see original*]

43 [*see original*]

44 [*see original*]

45 Thus, BSK-Stratenwerth, article 47 BA No. 7; Stocker, Regulatorische Anforderungen an IT-Outsourcing: Finanzmarktbereich, in: Weber/Berger/Auf der Maur (ed.). IT-Outsourcing 2003, 250 f. (under „presence of a certain need"). Otherwise Althaus Stämpfli, 224, which excludes outsourcing without permission from the bank's cost considerations; Berger, 191, according to which the interest of the bank in outsourcing is not sufficient in itself and in general and it is impossible to determine what interest of the bank in outsourcing outweighs the customer's interest in the protection of its secrecy; Aubert/Béguin/Bernasconi/ Graziano-von Burg/Treuillaud, 103, according to which outsourcing is permitted only if a bank is not able to perform the activity in question itself, which is to be assumed reluctantly.

(a) „Serve a genuine interest in optimization of their services or the reduction of their costs“;[46]

(b) Occurs „for reasons of division of labour and cost efficiency“,[47] as in the case of „the involvement of [...] software developers.“[48]

58 These limitations, however, are too narrow in our opinion. In terms of the law of obligations, in accordance with article 68 CO the basic – but dispositive – permissibility of outsourcing to service providers is to be assumed:[49]

[*see original*]

59 This also applies to banking activities. In fact, it follows from article 398 para. 3 CO that an „assignment“ (i.e. substitution) of the contract is impermissible, but that does not mean that any involvement of a third person is ruled out. The involvement of service providers in the sense of article 101 CO remains – in distinction to assignment of the principal performance obligations of a contract (substitution) – to a large extent permissible.[50] For example, even a surgeon who is personally obligated to perform is entitled to call in an „anaesthesia nurse“ „so long as the material main focus remains on his service“, „oversight and control by the obligor also [being sufficient], depending on the specific circumstances [...]“[51]. Accordingly, it (also) follows in the case of banks that outsourcing to a service provider is permissible under civil law, if:

(a) The outsourcing conforms to a reasonable interest of the outsourcing bank;

(b) The outsourcing is to be understood as the involvement of a service provider, i.e. the service provider's activity supports the bank's business activities and is subject to its instruction; and

(c) The bank itself renders the preponderance of the total services agreed to with the bank's customers.

---

46 [*see original*]
47 [*see original*]
48 [*see original*]
49 [*see original*]
50 [*see original*]
51 [*see original*]

60 So long as these conditions are satisfied, the involvement as such is not only permissible under contract law (subject to an agreement to the contrary), but also does not violate the protection of secrecy as a personal right.[52] It also follows from this that bank client confidentiality merely strengthens through the criminal law the confidentiality obligation based on civil law (see para. 14 et. seq. above), which is why nothing else can apply under criminal law other that what applies under article 68 CO, especially since article 47 para. 1 BA uses the term „agents", but does not restrict the scope of the term agent.

61 In the case of permitted assistance, there is no obligation that the bank release itself on a case-by-case basis through a waiver or in general from bank client confidentiality.[53] It is not that the violation of confidentiality is justified, but rather that the elements of unlawful disclosure are absent.

62 However, this is subject to the reservation that it does not follow from an agreement – express or tacit – that the involvement is not permitted. If a contractual agreement provides for the prohibition against making CID known abroad, compliance with this agreement is also protected under criminal law by article 47 para. 1 and 2 BA. In such a case, a disclosure abroad requires the prior consent of the customer covering the specific instance (a waiver) or a prior amendment to the corresponding contractual provision. As to the question of whether the exclusion of disclosure abroad was agreed to, not only any express agreements of the bank with its customers are to be considered (e.g. the corresponding provisions in the general terms and conditions), but also all other circumstances that taken together allow one to conclude that there was a corresponding commitment by the bank (which can be tacitly assumed under article 6 CO), as well as the bank's demeanour and market position, its statements regarding data protection and, to a certain extent, the industry practice.

4.2. Permissibility of outsourcing to foreign countries

63 Article 47 para. 1 BA also does not expressly prohibit data outsourcing to foreign countries. The legislative materials also contain no reference to a corresponding criminal liability. The literature, however, contains the opinion that the outsourcing of CID abroad results either legally (cf. para. 43 et. seq. above)

---

[52] If the bank does violate a provision of data protection law, e.g. the obligation of transparency in connexion with the assistance, this will serve as a violation under article 12 para. 1 FDPA, but it cannot be inferred from this that this makes the disclosure attendant on the involvement of the service provider impermissible as such.

[53] Issues of the transparency that may be required by data protection law are not the subject of this opinion.

or factually in a lapse of the protection provided bank customer confidentiality under the criminal law and the bank customer may assume from this that a violation of the confidentiality obligation entails criminal penalties. Therefore, outsourcing abroad requires consent.[54]

64 In fact, this view is supported by the fact that article 47 para. 1 and 2 BA threatens violations of confidentiality with punishment. Obviously, the legislature considers it necessary for the protection of the bank customer to subject the holder of the secret to criminal liability. This legislative judgment cannot be an unimportant one, particularly since in an earlier time the threatened punishment was even more severe (see para. 20 above). Nevertheless, the conclusion that outsourcing to an agent in a foreign country is prohibited without distinction is too undifferentiated. In the first place, there is no clear support for this in article 47 BA, so that the disclosure to a service provider abroad cannot be excluded in principle simply on the basis of the legality principle (article 1 CC). Moreover, the considerations that are important in the case of outsourcing to a service provider in Switzerland must also be given weight in the case of foreign disclosure (see para. 47 et. seq. above). It must therefore be assumed that the involvement of a service provider abroad is also permissible. Here again, the bank must observe the duty of care required by the circumstances, which raises additional questions in the case of disclosure abroad (see para. 65 et. seq.).

4.3. Conclusion

65 The bank may transmit CID to a service provider if the involvement serves a reasonable interest of the bank and does not violate any agreement with the bank's customer. In principle, this also applies with regard to a service provider abroad. In this connexion, it is not necessary that the CID be encrypted so that the service provider cannot have knowledge of the CID. The bank is criminally liable under article 47 para. 1 and 2 BA only:

(a) If it discloses CID, without the consent of the bank customer, to a person that is not an agent, but a third party; or

[54] [*see original*]

(b) If it fails to take required risk-mitigation actions and thereby causes the CID to come to the knowledge of an unauthorised third person, provided that in doing so the bank has acted (contingently) intentionally or negligently (see para. 39 f. above). We go into this in the following section.

5. Standard of care in outsourcing

66 In the case of assistance by service providers, the bank is obligated to exercise the care required by the circumstances. If it violates this duty of care and this results in a disclosure of CID by the service provider to an unauthorised person that is caused by the lack of due care, this may constitute an intentional or negligent violation of article 47 para. 1 and 2 BA.[55]

67 The question is what care is „required by the circumstances" (article 12 para. 3 CC). This question would be determined in the specific case by the criminal judge. In doing so, the judge has discretion, and the danger always exists that it will be concluded directly from the unauthorised disclosure that there has been a violation of the duty of care, which would of course be inadmissible.

68 Also relevant is the fact that, with regard to each case, it must be considered in the first place who violated the duty of care and whether an unauthorised risk was even created (see para. 40 above).

69 For the purposes of specificity, the court must proceed first of all from the relevant legal provisions regarding the duty of care. Also of importance are the generally recognised recommendations, guidelines, leaflets etc. issued by private and public authorities.[56] In this connexion, the following sets of rules may be of particular (but not exclusive) importance:

(a) The requirements of Swiss data protection law regarding data security (cf. article 7 FDPA, article 8 et. seq. of the ordinance to the FDPA), which requires compliance with the „current technical state of the art" (article 8 para. 2 lit. d of the ordinance to the FDPA).

[55] Further obligations of the bank arise, as applicable, from the provisions related to protection of secrecy, such as under article 162 or article 273 CC and applicable data protection laws.

[56] [*see original*]

(b) As applicable, the requirements of Swiss data protection law regarding the cross border transfer of personal data (article 6 FDPA, article 5 et. seq. of the ordinance to the FDPA).

(c) The requirements of Circular Operational Risks, annex 3 (handling of electronic customer data).

(d) The FDPIC's guide for technical and organisational measures on data protection, insofar as these guidelines contain recommendations on the application of certain technical and organisational measures (**TOMs**).

(e) As applicable, further relevant technical standards, insofar as they relate to the current state of the art.

70 These standards require first of all the collection and assessment of the risks associated with outsourcing. Under this heading, the bank must in general evaluate the following areas, for example:

(a) The risks to data security existing in the specific case, including the effect of appropriate mitigating technical and organisational actions by the bank and its service provider, such as, for example, encryption (taking into consideration code management and contractual requirements and prohibitions placed on the service provider) (see para. 24 et. seq. of the Guidelines).

(b) Other risks specific to the service provider that are to be evaluated in connexion with the selection and contracting process, mitigated through appropriate TOMs and/or accepted, including the inclusion of subcontractors and support in the case of a migration (see para. 13 et. seq. of the Guidelines).

71 The bank must reach additional appropriate contractual understandings with the service provider and supervise and, if necessary, enforce their observance (see para. 12 of the Guidelines).

72 In the case of outsourcing abroad – or if potential of access to CID is granted abroad, which is to a great extent the same thing – specific foreign risks are to be taken into consideration as well, in particular:

(a) At what site is CID stored or can be stored during the period of the contract or the processing and from where is access possible.

(b) In the case of violation, what are the legal risks for the service provider under the applicable local law, e.g. any criminal penalties, and the associated risk that the foreign service provider will not act with the same care as a service provider engaged in Switzerland because the risk of prosecution is absent or is less. Here, however, it would be unrealistic to assume that only the criminal penalties under article 47 para. 1 and 2 BA might prevent a service provider from passing CID on to an unauthorised third party. The risk to reputation may weigh more heavily, at least in the case of providers operating worldwide that would fear enormous losses if an unauthorised disclosure of CID became known. Moreover – but perhaps of lesser importance – the barriers of local law are of consequence, such as § 203 of the German Criminal Code or threat of fines under the European General Data Protection Regulation (article 83 GDPR).

(c) The legal and actual possibility of access by local authorities at the relevant sites and the risks to the bank's customers arising from this access[57]

(d) The ability of the bank and its customer to employ legal means to fight back against such access (since the risk of an access in connexion with a legal proceeding also exists in the case of data located in Switzerland and outsourcing abroad is not prohibited per se and grounds for justification are also conceivable in the event of an appropriate request, the bank typically satisfies its duty of care in this regard when it has ensured that it and/or the affected bank customer can have an appropriate request reviewed in a legal proceeding).

(e) The legal and actual potential of access triggered by the specific outsourcing by authorities other than those of the site in question, for example within the scope of a court order, that requires disclosure of data stored outside the territory in question. This is the case, for example, with the US CLOUD Act, which included the following provision in the Stored Communications Act (section 103(a)(1)):[58]

[57] The risk in general of access to CID by a government authority also exists in Switzerland and in principle does not violate bank client confidentiality. In this regard, consideration should be given only to the additional risk arising for a bank customer that *a foreign* or *the specifically responsible foreign* authority will access CID.

[58] [*see original*]

[*see original*][59]

(f) The risk that local authorities may access CID in violation of legal principles, whereas the risk of such access for purely fiscal or political reasons is regarded as more severe than an access based on reasonable suspicion of criminal activity.

(g) The available information making it possible to evaluate these foreign risks.

73 These risk assessments, considerations, conclusions and actions should be documented and, as necessary, updated.

74 In there is a violation of the required duty of care, the statements previously made in para. 39 et. seq. and para. 65 are particularly valid. In addition to these duties of care, the bank may be bound by other provisions, in particular other provisions relating to the protection of secrecy and the applicable data protection law that are not the subject of the present opinion.

[59] However, insofar as the data concerns persons who are neither US citizens nor reside in the United States, the handover of the data can be prevented in court if the country in which the data is held has concluded an executive agreement with the United States; cf. *Determann/Nebel*, U.S. CLOUD Act – Clouds Over the Basic Data Protection Regulation?, in: CR 6/2018, 408-412, 410.