VISCHER

Does a cloud solution meet the requirements of a Swiss bank[1]?

by David Rosenthal (drosenthal@vischer.com)

Requirement	CID (professional secrecy)	Personal data (Swiss DPA)	Relevant factor for TIA[2]	Essential outsourcing [3]	Core operational data [4]	Core application	Secondary application	Type / No. Requirement
Data at-rest in Switzerland The content data[5] is (only) stored on servers in Switzerland. However, this is no statement about the processing location.	P		✓			P		A01
Data at-rest in Europe The content data is (only) stored on servers in Europe. However, this is no statement about the processing location.		X	✓			X		A02
Processing only in Switzerland In principle, the provider only processes the content data in Switzerland, i.e. there is no automated or manual access from outside, except in exceptional situations.			✓			P		A03
Processing only in Europe In principle, the provider only processes the content data in Europe (but not necessarily in Switzerland), i.e. there is no automated or manual access from outside, except in exceptional situations.			✓			P		A04
Data at-rest encrypted When in a "dormant" state (i.e. when stored), content data is encrypted using state of the art encrypted.	X	X	✓					K01
Access to keys controlled by bank The key required for decrypting the content data at-rest is in principle only available to those users or applications/processes that the customer has authorised. The customer can monitor the authorisations.	X	P	✓					K02
Key is with provider, but managed by bank	P		✓					K03

[1] Similar requirements apply to other regulated financial services institutions and institutions that are subject to professional secrecy.

[2] Transfer Impact Assessment (for determining the risk of a foreign lawful access).

[3] According to FINMA Circular 2018/3 ("Outsourcing"), para. 4 ("Significant functions are those that have a material effect on compliance with the aims and regulations of financial market legislation").

[4] Data required for the restructuring or resolving the bank (Outsourcing Circular, para. 31)

[5] This refers to content data of the respective application, e.g. the client-identifying data of the bank managed by using the application. It does not mean the usage data or user account data in connection with the application's use.

The key required for decrypting the dormant content data is kept at the provider (key store), but the key management is (remotely) performed by the bank. It can give instructions to generate, replace and revoke keys.								
Key only at the bank The key required to decrypt content data at-rest is stored in a key store in the hands of the bank and not the provider. The bank also operates the key management.			✓					K04
Data in-transit encrypted When accessing the cloud-based solution, any transmission of data is encrypted.	X	X	✓					K05
Adequate, state-of-the-art data security The measures taken by the provider to ensure the data security of the cloud-based solution are state of the art and are adequate in view of the required level of protection in the specific case. The data security measures are regulated in a security policy (at least the "TOMS"). A risk analysis has been performed and did not result in unacceptable high risks.	X	X	✓	X	X	X	X	S01
Access for users only with MFA Access to the cloud-based solution, with or without access to the content data, is secured with multi-factor authentication.	X	X						S02
Data security tested and documented according to SSAE 18/ISAE 3402 SOC 1 & 2 Type II Test reports in accordance with SSAE 18/ISAE 3402 are available for all systems and processes relating to the solution, which also confirm the effectiveness of the controls (Type II). The provider undertakes to provide them.	X	X	✓	X	X	X	X	S03
Provider reports cyber attacks immediately If there is a cyber attack on the solution that affects the data security of the content data, the provider is obliged to report this to the bank immediately and to support it in fulfilling its reporting obligation to FINMA[6].				X		X	X	S04
Bank can access customer data and solution at any time The provider undertakes to provide the bank with access to its content data and the functionality covered by the solution at all times. There is an appropriate service level agreement.				X	X			B01
Copy of operational core data in Switzerland The solution ensures in one way or another that a copy of the data processed with the solution is kept on Swiss soil. This applies both to data that is essential for to be able to conduct its business and to the data and software required to access the data in a useful form.					X			B02
Backups of data ensured It is ensured that the data required for the operation of the solution is backed up should the system used for the operation of the solution fail or be destroyed or should the data be deleted or its integrity be impacted. This can be achieved by use of backups, but also mirrors.		X		X	X	X		B03
Continuation of business ensured even in the event of solution failure		X		X	X	X		B04

[6] FINMA supervisory communication 5/2020 on the specification of Art. 29 para. 2 FINMASA.

In terms of business continuity management, it is ensured that in the event of a failure of the system used for the operation of the solution, the continuation of the solution or otherwise the continuation of the bank's business is guaranteed. This can be done, for example, by means of a mirror. A risk analysis has been performed and did not result in unacceptable high risks.								
Orderly repatriation of the outsourced area possible within notice period It is possible that the area or function of the bank covered by the solution can be transferred to another provider or back to the bank within the agreed normal notice period.				X	X	X		**B05**
Continuation of service assured in case of failed repatriation The provider undertakes to continue to operate the solution for at least twelve months if the repatriation should fail for any reason.				X				**B06**
Continuation of service in the event of bankruptcy of bank In the event of bankruptcy or insolvency of the bank, the provider undertakes to transfer the contract to a third party who will take over the bank's business, provided that the third party pays the costs.		X		X	X	X		**B07**
Access to content data in the event of bankruptcy of the provider The bank's access to its content data is in principle provided for even in the event of bankruptcy of the provider.				X		X		**B08**
Written contract The rights and obligations of the parties and their responsibilities are documented in a contract. The form contract shall permit proof of its content in text form, but may be electronic.	X	X	✓	X		X		**C01**
Bank has right of instruction to provider The provider grants the bank a right to issue instructions, which can, however, also be "standardised" in that the instructions result from the content of the contract and the customer configuration. In the case of a data processing agreement pursuant to art. 28 GDPR, the right to issue instructions is included with reference to the processing of personal data.			✓	X		X		**C02**
Data processing agreement according to art. 28 GDPR The provider concludes a data processing agreement with the bank in accordance with the requirements of art. 28 of the GDPR.	X	X	✓	X				**C02**
Data processing agreement refers to Swiss DPA The data processing agreement stipulated for by the provider (and the other provisions on data protection) refer to the Swiss DPA (not only the GDPR) and also apply where only the Swiss DPA applies.		X	✓	X				**C03**
Data processing agreement also applies to CID (not only personal data) The rules provided in the data processing agreement apply not only to personal data (i.e. data of natural persons) but to all content data or CID (including those of legal persons).	X		✓	X				**C04**

Bank has a right to object to the use of material subprocessors Insofar as the provider uses subprocessors who do not process personal data (the data processing agreement applies there), the provider shall grant the bank a right of objection if they are to provide significant parts of the service. If subcontractors always (also) process personal data anyway, this is already included in the data processing agreement pursuant to art. 28 GDPR.			✓	X				**C05**
Content data may either not be used for provider's own purposes or the data processing agreement must apply mutatis mutandis Insofar as the provider reserves the right to process content data for its own purposes (e.g. billing, statistics), the same measures (data security, regulations on the involvement of third parties, audit right, etc.) shall apply as provided for in the data processing agreement. Access to CID (in cleartext) by employees of the provider for provider purposes that are not needed for performing the contract are prohibited.	X		✓	X				**C06**
Indefinite obligation of provider to maintain confidentiality of content data The provider undertakes that it and its employees will maintain the confidentiality of all content data. This confidentiality obligation is perpetual. Exceptions are limited to disclosures required by law.	X	X	✓	X				**C07**
EU standard contractual clauses used in case of access from outside Europe Insofar as the provider accesses personal data from non-whitelisted country, it undertakes to sign the standard contractual clauses of the European Commission (or BCRs approved in accordance with the Swiss DPA/GDPR). If a subprocessor is in a non-whitelisted country, then the standard contractual clauses shall be entered into between the provider and the subprocessor (not necessarily the bank).		X	✓	X				**C08**
If provider processes employee data for its own purposes, it shall comply with data protection If the provider processes employee data for its own purposes, it undertakes to provide for an adequate level of data protection and to process that data to the extent possible only pseudonymized, in a proportionate manner and for non-personal purposes (e.g., no direct marketing). The adequacy of data protection is determined by European standards.		X	✓					**C09**
"Defend your Data" obligation for foreign lawful access If the provider is confronted with disclosure orders from foreign authorities or courts in relation to content data, it will legally defend itself against these as far as reasonably possible. This also applies with regard to authorities within the EEA, not only those outside Europe.	X	X	✓	X				**C10**
Provider must be reasonably liable for breach of contract The contract with the provider provides for the reasonable liability of the provider (at least direct damages up to the amount of an annual fee). No exclusion or limitation of liability for gross negligence or wilful intent of the provider or its helpers, in particular not where applicable law permits such exclusions and limitations (e.g., Irish law).	X	X	✓	X	X	X	P	**C11**

No uncontrolled contract changes It must not be possible for the provider to unilaterally adjust the contractual provisions for the protection of the data processed with the solution and for the fulfilment of the regulatory requirements (insofar they weaken the protection); otherwise the bank has the option to exit from the solution.	X	X	✓			X		**C12**
Entitlement to contract adjustment (or exit) for legal reasons Should a legal development make it necessary to adjust the contract with the provider, the provider will negotiate this with the bank in good faith. If they cannot reach an agreement, the bank can exit from the solution.				X		X		**C13**
No relevant risk of foreign lawful access The probability of a foreign lawful access with and without the possibility of a legal recourse has been determined for the case at issue and a defined period of time on the basis of a Transfer Impact Analysis (TIA). A statistical method for determining such probability exists for this purpose.[7] The probability should be less than ten percent; access must be "highly unlikely" for the specific case of transfer.	X	X	n.a.	P	P	P		**C14**
Representations made by bank to customers are not violated Statements in GTCs, privacy notices and contracts must not contain any promises or statements that conflict with the outsourcing.[8]	X	X						**C15**
Outsourcing is regulated internally The use of the solution is governed by the internal regulations for outsourcing projects and there are corresponding responsibilities.				X				**C16**
Data security audit regularly (at least on a delegated basis) The data security of the solution is regularly checked by an independent, qualified auditor. The audit report (not only the certification or audit confirmation) is available to the bank in a meaningful form. Deficiencies are addressed.	X	X	✓	X		X		**P01**
Audit of the outsourced area, including access to data (without limitations, also on site) The bank, its external audit firm and FINMA can audit in full the outsourced area at any time and without hindrance, including on site.				X				**P02**
Provider must provide FINMA with all the information and documents it requires. The provider, which is not itself subject to FINMA, must be contractually obliged to provide FINMA with the information and documents required for supervision purposes.				X				**P03**
FINMA and the external audit firm can directly contractually enforce audit and information rights				X				**P04**

[7] https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx.

[8] Statements such as that no customer data can be accessed in plain text from abroad, when in fact this is possible.

The audit firm and FINMA can contractually (as a third-party beneficiary right) enforce their audit and information rights directly against the provider, even abroad and under the chosen law. They have their own access right to any audit reports prepared on behalf of the provider.								
Each group company can contractually directly enforce performance, audit and access rights Group companies that do not have a direct contract with the provider but nevertheless use the solution can contractually (as a third-party beneficiary right) enforce the contract's performance as well as their audit, information and access rights against the provider, even abroad and under the chosen law.				X				**P05**

Legend: X = Required P = Psychologically required (= Business Decision)

Requirement classification:

A = Architecture K = Cryptography S = Security

B = BCM C = Compliance P = Audit rights

Note: For legally compliant outsourcing, other requirements must be met within the institution (such as correct integration into the internal control system, the obligation to inventory, the monitoring of the provider, the appropriate configuration of the solution, etc.). These are not listed here.