This Q&A provides jurisdiction-specific commentary on Standard document, Personal data processing agreement: Cross-border (w-006-7129).

REGULATORY REQUIREMENTS AND WRITTEN AGREEMENTS

1. Do your data privacy laws require organisations to execute written personal data processing agreements before sharing or transferring personal data to third parties? If so, describe any situations when the parties would need to obtain regulatory approval or disclose the agreement terms to regulators, data subjects or other parties.

Article 10a of the Swiss Federal Act on Data Protection (Swiss FADP) permits outsourcing personal data processing to third parties if the outsourcer first establishes a data processing agreement. Strictly speaking, this agreement does not need to be in writing, although, in practice, written form is highly recommended for evidentiary purposes.

Further, if the outsourcing arrangement involves a cross-border personal data transfer to a country not ensuring adequate data protection and contractual guarantees serve as the legal basis for such transfer, these guarantees are usually also recorded in writing. Data controllers must also notify the Swiss Federal Data Protection and Information Commissioner (Swiss FDPIC) of any contractual guarantees for these cross-border personal data transfers (see Country Q&A, Data protection: Switzerland: Cross-border transfers of personal data (w-009-5012)).

For an overview of Switzerland’s data protection laws, see Country Q&A, Data protection: Switzerland.

DATA CONTROLLERS AND PROCESSORS

3. Do your data privacy laws impose different obligations or liabilities on data controllers and data processors? If so, describe those different obligations and liabilities.

The Swiss Federal Act on Data Protection (Swiss FADP) does not distinguish between the concepts of “data controller” and “data processor” in the same way as the EU’s data protection law. While Swiss law recognises that organisations can delegate personal data processing to a third party acting on its behalf, this does not relieve the third-party processor from meeting most of the Swiss FADP’s obligations (Article 10a, Swiss FADP). However, some obligations are only incumbent upon the person known as the “controller of a data collection,” which Swiss law defines as the person that decides on the data collection’s purpose and content (Article 3(j), Swiss FADP).

Obligations that only the controller of a data collection must observe include:

- The obligation to grant access to a data subject’s personal data (see Country Q&A, Data protection: Switzerland: Question 20 (w-009-5012)).
- The obligation to register data collections with the Swiss Federal Data Protection and Information Commissioner (Swiss FDPIC).
- The obligation to provide specific information when collecting personality profiles or sensitive personal data (see Country Q&A, Data protection: Switzerland: Question 8 (w-009-5012)).
RECORDKEEPING REQUIREMENTS

4. Do your data privacy laws place any specific recordkeeping requirements on service providers, such as maintaining detailed records of processing activities? If so, describe those requirements.

The Swiss Federal Act on Data Protection (Swiss FADP) does not require recordkeeping in the traditional sense. However, according to the Swiss FADP’s implementing legislation, if one processes sensitive personal data or personality profiles by automated means and the general data security measures do not sufficiently ensure data security, the controller of the data collection must implement a log file system to track the processing of personal data (see Country Q&A, Data protection: Switzerland: Question 25 [w-009-5012]). For more on Switzerland’s general personal data security requirements, see Country Q&A, Data protection: Switzerland: Data Security (w-009-5012).

EMPLOYEE BACKGROUND CHECKS

5. Can organisations contractually require their service providers to conduct background checks or any other reasonable steps to ensure the reliability and integrity of any employee handling personal data for the organisation?

Yes. In Switzerland, organisations can contractually require their service providers to conduct background checks. However, the contract should clarify that all background checks the service provider performs must meet the requirements and limitations of the applicable employment law.

EEA PERSONAL DATA TRANSFERS

6. Do service providers based in your country need to execute Standard Contractual Clauses before they can import personal data originating in the European Economic Area (EEA)?

No.

SUBCONTRACTORS

7. Do your data privacy laws restrict or place any requirements on a service provider’s use of subcontractors?

Yes. A service provider’s appointment of subcontractors generally requires the customer’s consent, although the customer can provide a general consent.

MATERIAL BREACH

8. Do contracts in your country use the concept of material breach to allow immediate termination of the agreement? If not, what language do contracts in your country commonly use to permit termination for a serious breach?

“Material breach” is not a term of art under Swiss contract law. Still, it is widely used in contracts subject to Swiss law and a Swiss court or arbitrator would likely construe the term to mean a breach of contract that substantially deprives the non-breaching party of what it was entitled to expect under the contract.

AUDITS

9. Do your data privacy laws require organisations to audit service providers who process personal data on their behalf?

The Swiss Federal Act on Data Protection (Swiss FADP) does not specifically require the customer to audit its service providers. However, the customer is under a general obligation to verify that personal data service provider only processes personal data in accordance with the customer’s instructions and an audit right is one method of implementing this in practice.

INDEMNIFICATION

10. Do your data privacy laws hold an organisation responsible or liable for its service provider’s data protection violations? If so, may an organisation require indemnification against potential damages and costs from its service provider?

Yes. Organisations are generally liable under the Swiss Federal Act on Data Protection (Swiss FADP) for privacy infringements committed by their service providers, and sanctions for such infringements can be imposed both on the organisation and its service provider. For more on the Swiss FADP sanctions, see Country Q&A, Data protection: Switzerland: Question 5 (w-009-5012). The organisation can require the service provider to grant an indemnity holding it harmless if the service provider breaches any data protection requirements.

SENSITIVE PERSONAL DATA

11. If the processing arrangement involves sensitive personal data, what, if any, agreement revisions should the parties make to Standard document, Personal data processing agreement: Cross-border (w-006-7129)?

As a matter of law, no specific adjustments are necessary. For more on the Swiss FADP sanctions, see Country Q&A, Data protection: Switzerland: Sensitive Personal Data (w-009-5012).

THE PROCESSING AGREEMENT

12. Does Standard document, Personal data processing agreement: Cross-border (w-006-7129) contain any sections that are not legally valid as drafted or not standard practice in your country? If so, identify the changes required to bring the personal data protection policy into compliance with your country’s applicable law and standard practice.

Organizations operating in Switzerland should consider revising Section 1.1 of Standard document, Personal data processing agreement: Cross-border (w-006-7129) to mention legal persons, such as corporations, as potential data subjects. The Swiss data protection law applies to the personal data of both legal and natural persons.
13. What, if any, other sections or language do organisations in your country commonly include in a personal data processing agreement?

None. The provisions in Standard document, Personal data processing agreement: Cross-border (w-006-7129) are comprehensive and capture the provisions usually covered in Switzerland personal data processing contracts.

CONTRIBUTOR PROFILE

ALESSANDRO CELLI, PARTNER
Baker & McKenzie Zurich
T +41 44 384 13 66
E Alessandro.Celli@bakermckenzie.com
W www.bakermckenzie.com
Areas of practice: Information technology & communications.

SYLVIA POLYDOR, ASSOCIATE
Baker & McKenzie Zurich
T +41 44 384 14 14
E Sylvia.Polydor@bakermckenzie.com
W www.bakermckenzie.com
Areas of practice: Intellectual property.

SIMON ROTH, PARTNER
Lex Futura (formerly Senior Associate at Baker McKenzie Zurich)
E simon.roth@lexfutura.ch
W www.lexfutura.ch
Areas of practice: Intellectual property, data protection, and information technology.