Regulation on order data processing

Version September 2024

This provision describes the obligations of the contracting parties with regard to data protection. CYP fulfils certain orders for customers and in this context processes personal data within the guidelines of the Swiss Data Protection Act and/or the EU General Data Protection Regulation (together "Data Protection Provisions"). This regulation applies to all activities in connection with the concluded contract in which personal data ('data') of the customer is processed.

1. Role and responsibilities of the parties

In accordance with the data protection provisions, the client is responsible for data processing, while CYP is the processor. Both the client and CYP are responsible for full compliance with all data protection provisions applicable to them.

The client warrants and represents that it has informed persons about whom it provides CYP with personal data (or whose personal data CYP otherwise receives) about the processing by CYP in accordance with this provision in a comprehensive, comprehensible and easily accessible form and language and that, if necessary, these persons have consented to the corresponding processing or another justification is applicable.

Insofar as the client has a further obligation to provide information under the data protection provisions, it shall make this information available to the persons concerned.

The client also guarantees and assures that the processing by CYP in accordance with these regulations is carried out in compliance with the applicable data protection provisions and, in particular, does not go beyond the processing for which the client is authorised and does not conflict with any legal or contractual confidentiality obligations.

2. Subject and duration

The subject matter, duration, type and purpose of the processing are generally derived from the main contract.

The term of this provision is determined by the term of the main contract between CYP and the customer. Excluded from this are provisions of this regulation that entail additional obligations.

CYP shall process the personal data for as long as is necessary to pursue the purposes specified under this provision or to fulfil contractual and legal obligations, or longer if the corresponding personal data is subject to a statutory retention obligation or is required for evidence purposes.

As soon as the personal data processed under this regulation is no longer required, it will be deleted or anonymised by CYP. This does not apply to personal data that is stored by CYP in the course of normal operational backups.

The legal basis for the processing of personal data, if required by law, is the consent of the data subjects or the legitimate interest of the client in the commissioned data processing for the pursuit of the purposes described above.

The client is responsible for providing evidence of the relevant consent or legitimate interest in data processing by CYP. If a data subject withdraws consent or the legitimate interest ceases to exist, the client shall inform CYP accordingly without delay.

3. Categories of processed personal data

CYP processes the following categories of personal data:

- Personal master data (e.g. name, address, date of birth)
- Communication data (e.g. telephone number, e-mail address)
- Assessment, evaluation and training data

Persons concerned:

- Course participants
- Carers of course participants
- Company administrators
- Employees
- Interested parties

4. Instructions from the client

The data processing described in this regulation is deemed to be general processing instructions issued by the client to CYP for the processing of personal data. The instructions are set out in the contract.

Additional specific instructions regarding the processing of personal data to CYP will be implemented, provided that they are proportionate and involve reasonable efforts on the part of CYP.

5. Subcontractor and place of processing

CYP passes on personal data to third parties for subcontracted data processing ('subcontracted processors'). These sub-processors can be viewed on the CYP website at the following link: https://cyp.ch/en/data-privacy and are deemed to be authorised by the client upon conclusion of the contract.

The client also generally authorises CYP to engage additional subcontractors or replace existing subcontractors at its own discretion. CYP shall inform the client in advance of any addition or replacement of subcontractors. The client may object to this. If the client does not raise an objection within 10 days of notification, the addition/replacement shall be deemed authorised. In the event of an objection by the client, CYP may dispense with the consultation/replacement or propose an alternative and, if this is not possible or unreasonable, the corresponding service will be cancelled.

The processing of the order data takes place in Switzerland, within the EU, within the EEA or in a country which is assessed by the European Commission and the Federal Council as having an adequate level of protection and which offers an adequate level of protection of personal data within the meaning of the Swiss Data Protection Act. Any relocation of the commissioned data processing to a country outside this area may only take place with the prior consent of the client and in accordance with the applicable legal provisions (in particular in compliance with the conditions contained in Chapter V of the EU GDPR and the Swiss Data Protection Act). In such a case, the processor undertakes in particular to conclude suitable supplementary contracts before transferring or disclosing the commissioned data and, if necessary, to take appropriate legal, technical or organisational measures.

Sub-contractors are contractually obliged by CYP to adequately protect all personal data they receive in connection with sub-contract processing and to use it exclusively for the purpose of sub-contract processing.

6. Data security

CYP shall take all necessary technical and organisational measures to adequately protect the personal data processed under this regulation (in particular against manipulation, disclosure, loss, deletion or destruction). To this end, CYP issues directives, trains those responsible and implements appropriate security measures and IT and network security solutions.

CYP restricts access to personal data to those persons who need it to fulfil their duties and ensures that all employees, contractors or service providers involved in data processing maintain the confidentiality of personal data. The relevant persons must ensure compliance with this confidentiality obligation before commencing their activities.

7. Breach of data security

CYP shall inform the client as soon as possible if it discovers a breach of data security in accordance with the data protection provisions.

CYP shall support the client as far as possible and reasonable in dealing with the data security breach identified, on condition that the client compensates CYP appropriately for this.

CYP shall forward relevant information, where available, to the client for these purposes. The client shall remain responsible for its part for all necessary notifications to data protection supervisory authorities and data subjects. For its part, CYP shall report to the data protection supervisory authorities where a corresponding obligation exists.

8. Requests from affected persons

Persons whose personal data is processed under this regulation may assert their individual rights against both parties. If a person contacts CYP to exercise an individual right and CYP is not itself the processing party, CYP will forward the request to the client irrespective of the obligation to provide a follow-up service. The client shall respond to and handle such requests. At the request of the client and if available, CYP shall provide the client with the necessary information. The client shall ensure that the persons exercise any individual rights to which they may be entitled correctly and shall request such information as will enable the person to be identified without any doubts. CYP accepts no liability for incorrect or untimely responses.

9. Dealing with data protection supervisory authorities

If a data protection supervisory authority contacts CYP in connection with personal data processed under this provision, CYP shall forward the corresponding enquiry or order to the client, irrespective of the obligation to provide a follow-up service. The client shall correspond with the enquiring or disposing supervisory authority and answer its questions or comply with its order, in each case in consultation with CYP. At the request of the client and if available, CYP shall provide the client with the necessary information, see also section 7.

10. Liability and compensation

The client and CYP shall be liable to data subjects in accordance with the statutory provisions of Art. 82 GDPR or the applicable provisions of Swiss law.

11. Notifications

Any communication from one party to the other under this provision shall be made in writing (including by email).

- for CYP: CYP Association, Giessereistrasse 18, 8005 Zurich / datenschutz@cyp.ch
- for the client: A person or body responsible for data protection enquiries will be named when the contract is concluded.

12. Applicable law and jurisdiction

This regulation is subject to substantive Swiss law.

The legal courts in Zurich, Switzerland, shall have exclusive jurisdiction over any disputes arising out of or in connection with this provision.

13. Final provisions

Each party shall be responsible for compliance with these provisions by its employees, contractors, agents and other third parties engaged by the respective party.

Any amendment or addition to these provisions must be made in writing in order to be valid and must expressly state that it is an amendment or addition to these terms and conditions.

Overview of technical and organisational measures

Access control

By means of access control, we take measures to prevent unauthorised access to data processing systems.

Measures

- User accounts and computers are secured by up-to-date and appropriate technical measures.
- Access from private smartphones requires a secure PIN and requires an up-to-date operating system.
- Mandatory use of password manager
- Access to office premises by means of door security and key logging.

Access control system

Access control system refers to measures that ensure that only authorised users can access the relevant data.

Measures

- Strict authorisation concept and regular review, also as part of audits
- Authorisation process for the release of access
- Administrative access is severely restricted to a defined group of people

Transfer control

The purpose of transfer control is to ensure that data cannot be read, modified or removed without authorisation during electronic transfer

Measures

- - Encryption of laptops via Bitlocker
- - Encryption of data transmissions (TLS/SSL)
- - Secured WLAN

Order monitoring

Order monitoring is defined as measures that ensure that personal data is only processed in accordance with the client's instructions.

Measures

- Data processing agreement (DPA) with service providers, if possible
- Regular review of data processors

Availability control

Availability control is a technical measure to restore stored data after data loss, damage or failure.

Measures

- Backup of data and services
- Locally separated storage of backups
- Threat protection
- Regular (at least 3 times a year) information and training of employees