Universität Zürich[UZH]

General Terms and Conditions of the University of Zurich for the Outsourcing of Data Processing using IT Services

(GTC UZH Data Outsourcing of IT-Services) Version January 2025[1]

1. Area of Application

These GTC form an integral part of the contractual relationship between the University of Zurich (mandator) and the service provider (mandatee), the subject of which is the outsourcing of the processing of personal and/or material data in accordance with § 6 of the Act on Information and Data Protection (*Gesetz über die Information und den Datenschutz*, IDG, LS 170.4) and in conjunction with § 25 of the Ordinance on Information and Data Protection (*Verordnung über die Information und den Datenschutz*, IDV, LS 170.41) using IT-services.

2. Responsibility

The mandator is responsible for the processing of the information.

The mandatee is only authorised to process the client's information within the scope of the contractual agreement.

3. Legal Power of Disposal over Information

The mandator retains full power of disposal over the processed information. In particular, the mandator may, at any time and without giving reason therefore and irrespective of the specific contractual situation, deny the mandatee access to the processed information, request the mandatee to return processed information in a previously agreed format at no cost, or require the mandatee to destroy the processed information.

4. Purpose Limitation

The information processed by the mandatee may solely be used for the purposes stipulated in the contract.

Any other uses must be authorised in writing by the mandator.

5. Disclosure of Information

Disclosure of Information to third parties shall be made only within the scope of the contractual agreement or if the mandator has given written consent.

Should the mandatee be obliged by a judicial enforcement measure to provide the relevant authorities with access to the mandator's systems and information, the mandatee shall inform the mandator immediately.

[1] The GTC UZH Data Processing by Third Parties are based on the GTC Data Processing by Third Parties («*AGB Datenbearbeitung durch Dritte*»), which were declared to be binding by the Government Council of the Canton of Zurich (Government Council Decision RRB 670/2015 dated 24.06.2015). These GTC are designed to ensure fair contractual relationships between public bodies as mandators and mandatees (e.g. providers of ICT services); in principle the GTC must be used to conclude new contracts.

6. Duties of Confidentiality

The mandatee, its employees, subcontractors and ancillary staff are subject to the comprehensive duties of confidentiality required by official secrecy during contract fulfillment and after contract termination.

Additional statutory duties of confidentiality (e.g. professional confidentiality) remain reserved.

Duty of confidentiality applies to all the mandator's systems, processes, and information; it applies equally within the mandatee's organization, irrespective of hierarchy.

Employees of the mandatee, the subcontractor or ancillary staff who process sensitive personal data within the scope of the contractual relationship are subject to the mandator's right of control and instruction, unless organisational and technical measures prevent them from gaining knowledge.

7. Requests for Access to Information

The mandatee shall forward requests for access to information as defined in § 20 IDG to the mandator. The mandatee shall take organisational and technical measures to enable the mandator to respond to such requests and to enforce the rights of data subjects to correction and deletion.

8. Information Security

8a. General provisions

The mandatee is aware of the mandator's duty to adopt suitable organisational and technical measures to protect information (§ 7 IDG). The mandator informs the mandatee about the protection requirements of the information to be processed [2]

To ensure the security of information, the mandatee maintains a data security management process that is graded according to the required level of protection. Th mandatee develops a data security organizational framework and a data security concept in order to maintain and continually improve information security within ongoing business operations. The ISO/IEC 2700-series standards or the "BSI Grundschutz"-standards100-1 to 100-4 apply.

8b. Separation of information

The mandatee shall take the necessary organisational and technical measures to keep the mandator's information separate from that of other clients.

8c. Mandatee's obligation to inform

The mandatee shall inform and document the mandator about the methods and processes it uses to ensure information security. The mandator has the right to view further documents and to have the operational procedures demonstrated.

Furthermore, the mandator must be informed immediately about any special incidents (loss of data, hacker attack, unlawful access). Formal reporting procedures via responsible contact persons must be determined.

[2] An overview of further measures required in different instances of data processing can be found in the Guideline on Processing Information under a Contract («Leitfaden Bearbeiten im Auftrag») by the Data Protection Commissioner of the Canton of Zurich, version V 1.14 / November 2023, page 11ff., and the Guideline on Encryption of Data Storage in the Context of Outsourcing («Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung») by the Data Protection Commissioner of the Canton of Zurich, V 2.3 / November 2023, and in the Guide for Technical and Organizational Measures of Data Protection («Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes») by the Federal Data Protection and Information Commissioner, dated January 2024.

8d. Logging
The mandator may require the mandatee to log each access to the information. The mandator has the right to inspect the logs

9. Monitoring

9a. Security Audits
The mandatee undertakes to have independent auditors periodically carry out security audits in accordance with recognized audit standards (for example those of the Swiss Institute of Certified Accountants and Tax Consultants or the Information Systems Audit and Control Association, ISACA). The mandatee furnishes the mandator with the reports on request, at no cost.

9b. Monitoring by independent Supervisory Authorities
Within the scope of the contractual relationship, the mandatee is subject to supervision by the mandator's supervisory body, in particular the Data Protection Commissioner of the Canton of Zurich and/or the Swiss Federal Audit Office. The mandatee must provide the mandator's supervisory bodies with access to its information, systems and processes, support these bodies at no additional cost and supply the necessary resources in terms of time and professional expertise.

10. Subcontracting

The mandatee is only permitted to use the services of subcontractors to fulfill its contract if the mandator has given his written consent or if the mandatee has disclosed this at the beginning of the contractual relationship. The subcontractor must legally assume all obligations arising from the contractual relationship and from these GTC.

11. System Development and Maintenance

If developing or maintaining systems requires the involvement of third parties, the mandatee adopts organizational and technical measures to prevent such third parties from gaining access to the mandator's information. If this cannot be prevented via organizational and technical measures, the provisions governing subcontracting apply.

12. Place of Data Processing / Equivalent Data Protection Level

The processing, retention and archiving of the mandator's information takes place in Switzerland as a general principle.

Personal data may only be processed outside Switzerland in a country with an adequate level of data protection (c.f. § 19 IDG in conjunction with § 22 IDV). The mandator must authorize this in writing. Documentation of the content and location of the information must be kept up to date.

13. Cloud Computing

When using cloud services, the following requirements must also be observed:
- The mandatee shall inform and document the mandator comprehensively and in writing about the technology used and any further development of the technology used.
- The mandatee shall inform the mandator of all possible data processing locations.

- All information containing sensitive personal data may only be transferred to the cloud with comprehensive cryptographic security. The mandatee shall ensure the necessary cryptographic measures are in place thoughout the entire processing procedure, including destruction. The client shall manage the necessary certificates (keys) itself.
- The measures for guaranteeing portability and interoperability must comply with the contractual agreement.

14. Safeguarding of the mandatee’s business secrets

The mandator undertakes to safeguard the mandatee's business secrets.
Legal duties of disclosure remain reserved.

15. Advertising

Advertising and publications about contract-specific services require the mandator’s written consent.

16. Sanctions / Penalties

In the event of a material breach of a provision of the contract or these GTC, the breaching party shall pay the injured party a contractual penalty, the amount of which shall be determined in accordance with the provisions of the General Terms and Conditions of the Swiss Conference on Informatics (SIK/CIS), January 2020 edition, unless it can prove that it is not at fault. The right to claim compensation for any further losses remains reserved. In the event of repeated serious breaches, the injured party has the right to immediately terminate the contract. The resulting damage is to be reimbursed to it.

Payment of a contractual penalty does not release the party from its confidentiality obligations.
Criminal sanctions remain reserved.

17. Termination of Contract

Regardless of the reason for the termination of the contract, the mandatee is obliged to transmit the information processed for the mandator free of charge and in the agreed format. The mandatee cannot delay this obligation, even if there is a dispute between the parties.

Upon termination of contract, the reasons therefore notwithstanding, the service provider undertakes to return the information processed on behalf of the client in the agreed format without delay and at no cost. The service provider may not defer fulfillment of this obligation, even if disputes arise between the contractual parties.

The mandator has the right to demand that the mandatee destroy the information processed within the scope of the contractual relationship free of charge. The mandator may have the fulfillment of this obligation checked by itself or by a third party.

18. Applicable Law

Swiss law applies exclusively.

19. Place of Jurisdiction

The exclusive place of jurisdiction is Zurich, Switzerland.