General Terms and Conditions of the University of Zurich for Outsourcing IT Services (GTC DP Outsourcing IT UZH)

Dated July 2018[1]

This is a translation of the original document in German. The translation is provided for information purposes only and has no legal bearing. Only the German document is legally binding.

1. Area of Application

These GTC form an integral part of the contractual relationship between the University of Zurich (client) and the service provider. When availing of IT services on behalf of the client, the service provider processes personal and/or non-personal 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).

2. Responsibility

The client is responsible for the processing of information.
The service provider is solely authorized to process the client's information in the scope of the contractual agreement.

3. Legal Power of Disposal over Information

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

4. Purpose Limitation

The information processed by the service provider may solely be used for the purposes stipulated in the contract.
Any other uses must be authorized in writing by the client.

5. Disclosure of Information

Information may only be disclosed to third parties if this is provided for under the contractual agreement or if the client has given written consent.
If the service provider is obliged to grant the competent public authority with access to the client's systems and information as the result of a judicial order, the service provider must inform the client without delay.

6. Duties of Confidentiality

Official secrecy is a statutory duty of confidentiality that applies to all members of a public authority and thus to all employees of the client. In the process of fulfilling their contractual obligations, the service provider, its employees, subcontractors, and ancillary staff act in the capacity of ancillary staff of the client. As such, they are subject during contract fulfillment and after contract termination to the same comprehensive duties of confidentiality as the client's employees, namely those required by official secrecy in accordance with Article 320 of the Swiss Criminal Code (SCC).
Additional statutory duties of confidentiality (such as professional confidentiality for doctors, dentists, and psychologists in accordance with Article 321 SCC, or professional confidentiality when conducting research on human beings in accordance with Article 321bis SCC, or that of manufacturing or trade secrecy in accordance with Article 162 SCC) remain reserved.
Duty of confidentiality applies to all the client's systems, processes, and information; it applies equally within the service provider's organization, irrespective of hierarchy.
Employees of the service provider, subcontractor, or ancillary staff who process personal and/or non-personal data as part of the contractual relationship are subject to the client's right of control and right of instruction.

[1] The GTC DP Outsourcing IT UZH serve to implement the GTC Outsourcing IT Services (*AGB Auslagerung Informatikleistungen*), which were declared to be binding by the Government Council of the Canton of Zurich in its official decision DGC 670 on 24 June 2015. These GTC are designed to ensure fair contractual relationships between public bodies as clients and service providers; the GTC must be used to conclude new contracts.

7. Requests for Access to Information

Requests for access to information as defined in § 20 IDG are forwarded by the service provider to the client. The service provider adopts organizational and technical measures to enable the client to respond to such requests and to enforce the rights of affected parties to have data corrected or deleted.

8. Information Security

8a. General Provisions

The service provider is aware of the client's duty to adopt suitable organizational and technical measures to protect information (§ 7 IDG). The client informs the service provider of the required level of protection for information to be processed.[2]

To ensure the security of information, the service provider maintains a data security management process that is graded according to the required level of protection. The service provider 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 27000 series standards or the *BSI Grundschutz* standards 100-1 to 100-4 apply.

8b. Separation of information

The service provider adopts the necessary organizational and technical measures to keep the client's information separate from that of other clients.

8c. Service provider's obligation to inform

The service provider informs and provides documentation to the client about the methods and processes it employs to enforce information security. The public body has the right to view further documents and to require a demonstration of operational procedures.

Furthermore, the client must be informed without delay about any security-related incidents (loss of data, hacker attack, unlawful access) that occur. Formal reporting procedures via responsible contact persons must be determined.

8d. Logging

The client has the right to ask the service provider to log each access to the information. The client has the right to inspect the logs.

9. Monitoring

9a. Security audits

The service provider 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 service provider furnishes the client with the reports on request, at no cost.

9b. Monitoring by independent supervisory authorities

Under the contractual relationship, the service provider is subject to supervision by the client's supervisory body, in particular the Data Protection Commissioner of the Canton of Zurich and/or the Swiss Federal Audit Office. The service provider must provide the client'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 service provider is only permitted to use the services of subcontractors to fulfill its contract upon receiving written authorization of the client. The subcontractor is legally bound to assume all obligations stipulated in the contractual relationship and in these GTC.

[2] An overview of further measures required in different instances of data processing can be found in the guideline Processing Information under a Contract ("*Leitfaden zur Bearbeitung im Auftrag*") by the Data Protection Commissioner of the Canton of Zurich, version V 1.4 / February 2018, page 12, and the Information sheet on encryption of data storage in the context of outsourcing by the Data Protection Officer of the Canton of Zurich, V 2.2 / June 2018 („*Merkblatt Verschlüsselung der Datenablage im Rahmen der Auslagerung*"),and in the Guide for technical and organizational measures by the Federal Data Protection and Information Commissioner, dated August 2015 ("*Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes*").

11. Systems Development and Maintenance

If developing or maintaining systems requires the involvement of third parties, the service provider adopts organizational and technical measures to prevent such third parties from gaining access to the client'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 client's information takes place in Switzerland as a general principle.

The processing of personal data outside Switzerland may only take place in a country with a commensurate level of data protection (c.f. § 19 IDG in conjunction with § 22 IDV); the written authorization of the client is required. Documentation of the content and location of the information must be kept up to date.

13. Cloud Computing

The additional following requirements must be strictly observed when using cloud services:

- The service provider informs the client in full and in writing and provides documentation about the technology used or about any further development of the technology used.
- The service provider informs the client of all possible data processing locations.
- To be stored in the cloud, all information containing sensitive personal data must be fully encrypted. The service provider ensures that the necessary cryptographic measures are taken during the entire handling process, including destruction. The client is responsible for the management of the necessary certificates (keys).
- Measures for guaranteeing portability and interoperability must comply with the contractual agreement.

14. Safeguarding Manufacturing and Trade Secrecy of the Client

The client undertakes to safeguard the service provider's trade secrets. Legal duties of disclosure remain reserved.

15. Advertising

Advertisements and publications that mention services specific to the contract require the client's written consent.

16. Sanctions/Penalties

In the event of a serious breach of a provision of these GTC, the faulty party must pay the injured party a contractual penalty equal to that stipulated in the provisions of the General Terms and Conditions of the Swiss Conference on Informatics (GTC CSI), version of January 2015, unless the accused party proves it is not at fault. Compensation for damage exceeding this amount remains reserved. The injured party reserves the right to terminate the contract immediately in the event of a repeated serious breach. Compensation must be paid for the damage arising.
Paying a contractual penalty entails no release from the duties of confidentiality.
Criminal sanctions remain reserved.

17. Termination of Contract

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 client has the right to demand that the service provider destroy the information processed under the contractual relationship at no cost. The client itself may verify whether this obligation has been fulfilled or engage a third party to do so.

18. Applicable Law

Subject to Swiss law.

19. Place of Jurisdiction

Place of jurisdiction is Zurich, Switzerland.