swisscom

Annex to the Data Processing Agreement

Data elements and technical and organisational measures (TOM) used

1 Data elements used

1.1 General

The Customer shall, at its own discretion and in relation to the contracts, provide Swisscom Broadcast Ltd (Swisscom) with personal data and/or confidential data for processing on its behalf.

1.2 Data subjects

The data may include personal data of the following data subjects in particular:

- Prospects, customers, business partners, sales people, and distributors of the Customer; all of whom are natural persons
- Employees or other auxiliaries of prospects, customers, business partners, sales people, and distributors
- Employees or other auxiliaries of the Customer whom the Customer has authorised to use the services

1.3 Types of personal data

The personal data to be processed may include the following in particular:

- Personal information, such as first name, last name, date of birth, age, gender, nationality, etc.
- Business contact details, such as e-mail address, telephone number, address
- Private contact details, such as e-mail address, telephone number, address
- Identity document details
- Career-related information, such as job title, role, etc.
- Information relating to an individual's private life, such as marital status, hobbies, etc.
- User information, such as login data, customer number, personnel number, user behaviour, etc.
- Technical information, such as IP address, device information, etc.

1.4 Sensitive personal data

This type of data pertains to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union affiliations, as well as genetic data and biometric data for the purpose of uniquely identifying a natural person, health data or data concerning an individual's sex life or sexual orientation.

1.5 Confidential data

Data that falls under this category may concern professional secrecy, banking secrecy, official secrecy or the duty of confidentiality under social security law.

2 Technical and organisational measures

2.1 General

1 The sections below describe the technical and organisational measures taken by Swisscom to protect personal data in the context of its data processing activities. The onus is entirely on the Customer to assess whether the measures described below are appropriate to protect the data entrusted to Swisscom for processing (in particular in the case of sensitive personal data or confidential data).

2 Swisscom maintains an Information Security Management System (ISMS) which complies with ISO27001 and other international standards.

3 The measures listed below are generic and apply only in the absence of explicit provisions in the contract, e.g. the specification of additional product or customer-specific measures or the express exclusions of any of the following measures. The following measures apply in cases where Swisscom itself processes the Relevant Data. If data processing is carried out by third parties commissioned by Swisscom, Swisscom shall ensure, through suitable contractual agreements, the third parties' compliance with equivalent measures.

2.2 Physical access control

1 Swisscom divides the areas within the building into security zones with different levels of security, namely: public, secure and high-security zones. Public zones are accessible to everyone; for example, the reception areas of an office building. For the secure zones, a badge or key is required to gain access. The badges of employees and service providers are personalised. A record is made of the issuing of keys to authorised persons. All visitors must be registered and accompanied by responsible employees within the secure zones. If non-personalised badges are used, a responsible person shall be appointed to keep a record of the temporary owners.

2 Swisscom data centres are classified as high-security zones. A high-security zone cannot be accessed directly from a public zone, but only via a secure zone. Access to the high-security zone requires two forms of identification and is logged. The data centres are owned by Swisscom or leased from third parties under a long-term lease.

3 Swisscom data centres have the necessary physical protective measures in place to detect a breach of the building perimeter and trigger an alarm at an early stage. In buildings that are manned around the clock, security staff are trained to process such alarms quickly and professionally and to initiate appropriate measures. If the buildings are not manned around the clock, the alarms are forwarded to a security service provider or the police to trigger an intervention.

4 Swisscom data centres have additional necessary protective measures in place to mitigate the risks posed by natural disasters such as lightning, rain, flooding, etc. to such an extent that they do not pose a threat to data centre operations.

5 If third-party data centres are used for the permanent storage of data for Swisscom services, Swisscom shall ensure that the operators of the data centre meet conditions comparable to those of Swisscom's data centres and thus guarantee an equivalent level of security.

6 If the Customer stores its data on its own premises, Swisscom can advise the Customer on how to secure these rooms. It is the Customer's responsibility to take the necessary protective measures.

2.3 System access control

1 Swisscom's systems can only be accessed by persons commissioned by Swisscom using personalised identification.

2 System access is always protected with at least one password or equivalent authentication feature and the associated digital identification. The access data is stored in such a way that no direct derivation of the valid authentication feature is possible should this data become accessible.

3 The passwords must meet complex requirements and include at least three of the following: uppercase letters, lowercase letters, numbers and special characters. Passwords of personal accounts are never made accessible to third parties.

4 In the event of incorrect login, the identification can first be suspended temporarily and then disabled permanently following further failed attempts.

5 Depending on the classification of users, portals accessible via the Internet require strong authentication when accessing the Relevant Data. The strong authentication is based on Mobile ID, the use of an electronic token to generate one-time passwords, or other secure means as a second factor.

2.4 Data access control

1 System authorisations have a role-based structure. An identity is assigned one or more roles that an individual requires to perform their organisational role. The roles are structured in such a way that an individual only has access to the data necessary to complete the task. A description of the roles and their respective authorisations are documented in role concepts.

2 Should an employee require additional rights, they can request an additional role. It is the responsibility of the line manager and the role owner to release this additional role. The role owner can decide whether, in fact, a release is required or whether the release can be automatic. A small number of roles are assigned to the employee automatically. These are roles from the organisational structure, such as assignment to an organisational unit.

3 Data traffic between the Customer's network and Swisscom is encrypted wherever possible or protected by alternative measures. Alternative measures include, for example, the use of dedicated logical lines or the use of direct fibre-optic connections. The encryption of the connection is based on current protocols and security mechanisms.

4 Access to the systems is logged and can be analysed using various methods.

2.5 Data transfer control

1 An encrypted connection is always required when accessing Relevant Data over the Internet. Swisscom uses up-to-date protocols and security mechanisms for this. This encrypted connection is based on network, session or application-layer technologies.

2 The Customer's direct access to its personal data shall be protected following agreement with the Customer about the data transfer route. Swisscom offers dedicated services that enable virtual network connections to the Customer. Other encryption techniques can also be used for these connections.

2.6 Storage control

1 Physical protection measures are used to protect the permanent data repositories in the data centres against loss. This includes redundant power supplies and the necessary systems to enable autonomous operation for a defined period of time.

2 To protect against smoke or fire damage, the high-security rooms are equipped with smoke detectors and fire alarm systems. In the event of an incident, either the on-site security or building personnel will be deployed for a first response or an extinguishing system will activate to keep potential damage to a minimum. If there is no personnel on site, the alarm will be forwarded to the local fire department.

3 Swisscom shall render faulty data carriers physically unusable to prevent any unauthorised access.

4 Functioning data carriers will be wiped using industry-standard deletion procedures so as to render reconstruction of the contained data almost impossible. If such a procedure is not possible, the data carriers will be rendered physically unusable or destroyed.

5 Data carriers may be returned to the Customer under defined circumstances. In such case, the storage system or data carrier must only have been used for that particular customer.

2.7 Data entry control

1 In the event that Swisscom is responsible for entering and processing personal data, Swisscom shall take the necessary measures to ensure that this data is collected and processed correctly.

2 Swisscom collects additional personal data of the Customer in Swisscom systems for the purpose of providing its service. These systems are used, for example, to log incidents and change requests or for invoicing. Swisscom shall use appropriate quality measures to ensure that Relevant Data collected in this way is verified and corrected.

2.8 Assignment control

1 Swisscom carefully selects all subcontractors who could potentially have access to the data and imposes the relevant data protection responsibilities on the suppliers.

2 Swisscom has appointed a responsible organisation for data protection matters. In case of enquiries, this can be contacted at datenschutz.sbc@swisscom.com. The first point of contact for questions about data protection at Swisscom is the responsible Swisscom Account Manager.

3 Before they start their employment, new Swisscom employees are subject to a security check of varying levels and forms depending on their opportunity to access Relevant Data. As a minimum, the check includes verification of the complete curriculum vitae and most recent certificates and receipt of a personal reference.
In subsequent stages, they may be required to sign a non-disclosure agreement or undergo personnel security screening pursuant to federal guidelines.

4 New employees are familiarised with the relevant rules for their own security and data security when they start work.

5 Existing Swisscom employees are regularly trained in the careful handling of data. This can be through notices on the Intranet, blog posts, electronic awareness training on Swisscom's learning platform and on-site training courses.

6 If a Swisscom employee leaves the company, their main identity on Swisscom's systems will be disabled automatically. Building access authorisation will also be revoked at the end of their last working day. It is the line manager's responsibility to revoke any other access authorisations and to confiscate the Swisscom badge and work equipment on the employee's last working day.

2.9 Availability control

1 In accordance with the contractual agreement, Swisscom stores the data in data centres with the necessary level of protection. (These may be Swisscom or third-party data centres).

2 Swisscom's storage systems are configured to ensure availability of the data even in the event of multiple component failure. This is achieved through redundant, distributed data carriers as well as redundant networks and power supplies.

3 Swisscom backs up the data in accordance with the service description. Backups can be made to storage systems situated in a separate data centre that is located a sufficient geographical distance from the original location. The purpose of the different geographical locations is to minimise the potential damage caused by natural disasters such as lightning, rain, flooding and mudslides to just one location, if possible.

4 Depending on the services purchased, the Customer can additionally order different backup levels. This is described in the service description or can be requested from Swisscom's account manager.

5 Swisscom has implemented the necessary processes to identify and evaluate reports of software vulnerabilities and patches, and derive the necessary further steps.

2.10 Separation requirement

1 Swisscom ensures that one customer's data is not visible to others. For this purpose, current security procedures are used which ensure the separation of customer data on a logical or physical level.

2 Physical procedures are appropriate when the service and the systems used do not allow adequate logical separation. For cost reasons, Swisscom always tries to use logical procedures wherever possible.

3 Depending on the service offered, the Customer can express the wish for its data be physically separated from the data of other customers. This option is not available with all services.

4 Logical procedures have been audited by Swisscom to ensure that these procedures cannot be rendered ineffective. If Swisscom finds that the procedures no longer guarantee this, Swisscom will take the necessary countermeasures to restore equivalent protection.

2.11 Auditing, assessment and evaluation

1 Swisscom conducts regular system audits. In the area of technology, for example, these include a regular audit of the IP perimeter or platform security audits.

2 New services are subjected to a technical audit based on a risk analysis. Identified deficiencies are remedied by the responsible parties. Depending on the severity of the deficiencies, a supplementary audit may be required to demonstrate the effectiveness of the remedy.

3 Swisscom maintains a risk management system throughout the company in order to identify and quantify risks and, together with the responsible organisations, to initiate measures to reduce risks.

4 Swisscom takes part in a Bug Bounty programme. This enables anyone to report centrally any detected security vulnerabilities in Swisscom's services. The reports are evaluated and the necessary countermeasures taken, e.g. a patch is created for software, or the code of a website is corrected.