swisscom

Annex to the Data Processing Agreement

Utilised Data Elements and Technical and Organisational Measures (TOM)

1 Data Elements Utilised

1.1 General

Within the scope of the contracts, the Customer shall provide Swisscom, at its own discretion and on its behalf, with personal data and/or confidential data for processing.

1.2 Data subjects

This may concern personal data of the following data subjects in particular:

- Potential customers, existing customers, business partners, vendors and distributors of the customer who are natural persons
- Employees or other auxiliary persons of potential customers, existing customers, business partners, vendors and distributors
- Employees or other auxiliary persons of the Customer authorised by the Customer to use the services

1.3 Type of personal data

This may concern the following types of personal data in particular:

- Personal information, such as first name, surname, date of birth, age, sex, nationality, etc.
- Business contact data, such as e-mail address, telephone number, address
- Private contact data, such as e-mail address, telephone number, address
- Details from identity documents
- Job-related information, such as job title, position etc.
- Information about the data subjects' personal life, such as marital status, hobbies etc.
- User information, such as log-in information, customer number, personnel number, user behaviour etc.
- Technical information, such as IP address, device information etc.

1.4 Personal data requiring special protection

These categories of data concern personal data that indicate the data subject's race and ethnicity, political views, religious or philosophical beliefs or union membership, as well as genetical data and biometric data for the unequivocal identification of a natural person, health data or data regarding the data subject's sex life or sexual orientation.

1.5 Confidential data

These data may concern data that are subject to, e.g. professional secrecy, bank-client confidentiality, official secrecy or the duty of confidentiality under social insurance law.

1.6 Delimitations

[1] If the data has been encrypted by the Customer and cannot therefore be viewed by Swisscom, it is not a case of commissioned data processing. The agreement on order data processing is therefore not applicable to this data.

[2] The assessment of whether the technical and organisational measures described below to protect the data entrusted to Swisscom for processing (namely in the case of personal data requiring special protection or data subject to secrecy) are appropriate shall be the sole responsibility of the Customer.

[3] Within the framework of the contractual relationship, each party processes personal data on employees and other auxiliary persons of the other party. This includes, for example, name, postal/email/IP address, telephone number, occupation/function, means of identification, copies of identity documents, etc. For the purposes of processing the contract and maintaining the contractual relationship (e.g. communication, access control, fault reports, orders, invoices, satisfaction analyses, information about new products, invitations to events, etc.), the parties process this personal data under joint responsibility on their own systems and using appropriate technical and organisational measures to protect the data. This type of data processing is not subject to the regulations of the agreement on order data processing, whereby Swisscom takes the following technical and organisational measures to protect this data.

2 Technical and organisational measures

The following chapters describe the measures taken by Swisscom with regard to the protection of personal data in context of order data processing. Swisscom maintains an Information Security Management System (ISMS) in accordance with the ISO27001:2013 standard. Swisscom's ISMS is certified; the certificate is available to the public on Swisscom's website (www.swisscom.com/datensicherheit).
The measures listed below are meant generically and are utilised unless otherwise determined in the respective contract, e.g. more extensive product- or customer-specific measures are specified or one or more of the following measures are explicitly excluded. The following measure apply to cases in which Swisscom itself processes the relevant data. If the data processing is performed by third parties on behalf of Swisscom, Swisscom ensures with suitable contractual agreements that the third parties apply similar measures

2.1 Admission control

[1] Swisscom divides its areas into different security zones. These zones are subdivided into public, secure, and high security zones. Public zones, such as the Swisscom Shops or the reception areas in an office building, are accessible to everyone. A badge or key is required in order to gain admittance to secure zones. Employees and service providers' badges are personalised. A record is made of the keys issued to authorised personnel. Visitors must register upon arrival and be accompanied by the responsible employees in the secure zones. If non-personalised badges are used, an officer is designated to keep a log of the temporary badge holders.

[2] Swisscom's computer centres are classified as high security zones. High security zone cannot be accessed directly from public zones but only through a secure zone. Access to the high security zone requires two-factor identification and is entered in an access log. The computer centres are owned by Swisscom or leased from third parties on a long-term basis.

[3] Swisscom's computer centres have the necessary physical safeguards in place to detect a breach of the building's perimeter promptly and trigger the appropriate alarm. For buildings that are staffed 24 hours a day, the security staff is trained to handle such an alarm swiftly and professionally and to initiate the proper measures. If the buildings are not staffed 24 hours a day, the alarms go to a security service provider or the police to trigger an intervention.

[4] Swisscom's computer centres also have further necessary safeguards in place to minimise hazards caused by natural phenomena, such as lightning, rain, flooding etc. such that they no longer pose an issue to the operation of these centres.

[5] If third-party computer centres are utilised for Swisscom services in order to permanently store data, Swisscom ensures that the operators of such computer centre fulfil conditions similar to those of its own computer centres so as to guarantee an equivalent level of security.

[6] If the Customer stores its data directly on site, Swisscom can make recommendations as to how to secure the relevant

spaces. However, the Customer is responsible for implementing the necessary safeguards.

2.2 Physical access control

[1] Physical access to Swisscom's systems can only be obtained with the personalised identification of Swisscom's authorised staff members.

[2] Physical access to the systems is always protected at least with a password or an equivalent authentication feature and the associated digital identification. The physical access data are stored such that the applicable authentication feature cannot be derived directly in the event that these become accessible.

[3] The passwords must fulfil complex requirements and are made up of at least three of the following types of elements: upper-case letters, lower-case letters, numbers and special characters. Passwords of personal accounts are never given out to third parties.

[4] In case of a failed login attempt, the relevant user's identification is blocked temporarily at first and, in case of additional failed attempts, it is blocked permanently. The user's identification can then only be unblocked by means of Swisscom's Service Desk. In this case, mobile ID is utilised to identify the user.

[5] If the user requires administration rights with a non-personal identity, the user must complete a "step-up" procedure: This means that the employee logs into the system with his/her personal account and then increases his/her privileges in the system. On Unix systems, this can be done, for example, by using the sudo command. If a step-up procedure is not possible, Swisscom can at any time employ its administration platform to determine which user has utilised the non-personal administration identity. All administrative accesses are centrally logged and stored at Swisscom for a defined period of time.

[6] Internet-accessible portals require strong authentication when accessing the relevant data, depending on the classification of users. In this case, the strong authentication is based on a mobile ID, the use of an electronic token to generate one-time passwords or other secure means as the second factor.

[7] Mobile ID is a Swisscom service based on a SIM card specifically adapted for Swisscom with a security module for cell phones and thus constitutes a secure identification for the user.

[8] Devices that obtain direct access to the company's network are identified via a machine-readable certificate. Employees who use personal device must log in over a virtual infrastructure to access the relevant customer data.

2.3 User access control

[1] Permissions on the systems are structured into roles. An identity is assigned one or more roles that are necessary for carrying out the person's organisational role. The roles are structured such that users can only access the data they need in order to perform the relevant task.

[2] A description of the roles and their permissions are documented in role concepts. These concepts are reviewed and updated on a regular basis. The roles concept is kept and updated by the system supervisor. All roles undergo a regular review to determine whether they are still required by the assigned users.

[3] If an employee requires more privileges, he/she can order an additional role. This additional role must be approved by the employee's supwervisor and the role owner. The role owner can decide if this approval is actually necessary or if the role can be released automatically. A very limited number of roles are automatically assigned to the employee; these are roles based on structure of the organisation, such as membership in an organisational unit.

[4] Access with enhanced privileges for administering Swisscom's systems only occurs via a dedicated infrastructure with strong authorisation. All logins, logouts and failed login attempts are logged centrally and stored for a defined period of time. In this case, the strong authentication is based on a mobile ID or the use of an electronic token to generate one-time passwords.

[5] Where possible, data sent between the Customer's network and Swisscom are transmitted in encrypted form or secured via other measures. Alternative measures include, for instance, using dedicated logical lines or direct optical fibre links. The encryption of the connection is based on current protocols and security mechanisms.

[6] System accesses are logged centrally, analysed using several different procedures and checked for information security breaches. Any breaches identified in this manner are analysed by a central team and the appropriate measures are taken.

2.4 Transport control

[1] Internet-based access to the relevant data is always achieved via an encrypted connection. For this purpose, Swisscom uses current protocols and safeguards. This encrypted connection is based on technologies on the network, session or application layer.

[2] The Customer's direct access to his/her personal data is secured based on the agreement made with the Customer as regards the transmission route. Swisscom offers the appropriate services to enable virtual network connections to the Customer. Other encryption technologies may also be used for these connections.

[3] To prevent the outflow of data, Swisscom has implemented safeguards at the e-mail and web interfaces that check whether large volumes of personal data are being transferred and thus constitute a potential outflow of these data into the Internet. The detected incidents are handled by a central team and aoccrding mitigating actions are implemented.

2.5 Storage control

[1] Physical safeguards are employed to protect the permanent storage in the computer centres from loss. These include redundant power supplies and the necessary systems to enable self-sufficient operation for a defined period of time.

[2] The high security rooms have smoke and fire alarm systems to protect against smoke and fire damage. In the event of an incident, the security personnel or building personnel present, as applicable, are utilised for a first response or an extinguishing system is activated to minimise the potential damage as much as possible. If no personnel are available on site, the alarm is directed to the local fire brigade.

[3] Defect data carriers are rendered physically unusable in order to completely rule out any potential access.

[4] Functioning data carriers are erased using standard deletion procedures so that it is virtually impossible to reconstruct the data contained in them. If such procedure is not possible, the data carriers are rendered physically unusable or destroyed, as applicable.

[5] Data carriers may be returned to the Customer under defined circumstances. This requires that the storage system or the data carrier, as applicable, was only in use for this one customer. In this case, Swisscom has a defined process for logging the data carriers and handing them over to the Customer in a Swisscom building.

2.6 Input control

[1] In the event that Swisscom is responsible for inputting and processing personal data, it takes the necessary technical and organisational measures to ensure that these data are entered and processed correctly. Technical measures are employed to verify the validity of the data, such as whether a reference to the person already exists in any other relevant system. Organisational measures for verifying accuracy may include, e.g. a follow-up check of inputs and adaptations or a sampling test of the data's accuracy.

[2] For purposes of providing its services, Swisscom records additional personal data of the Customer in Swisscom's systems. These systems are utilised, e.g. to record error messages (incidents) or change requests or for invoicing. Swisscom takes the proper quality assurance measures to ensure that the relevant data recorded in this process are checked and corrected.

2.7 Order monitoring

[1] Swisscom shall carefully select any potential sub-suppliers with access to the data and shall subject the suppliers to the relevant data protection responsibilities.

[2] Swisscom has designated a responsible organisation to ensure that the data protection requirements are met. Enquiries can be addressed to this organisation at datenschutz@swisscom.com. The first point of contact for issues regarding data protection at Swisscom is the responsible Account Manager of Swisscom.

[3] New Swisscom employees must undergo a security check before being hired. This security check is made up of several levels, and its design varies depending on the possibility of accessing relevant data. At a minimum, the check includes verifying the new employee's entire CV and his/her most recent school certificates, as well as obtaining personal references.
The subsequent stages include the signing of a confidentiality agreement and reviewing current extracts from the Register of Criminal Convictions and the Debt Enforcement Register.

[4] When beginning their employment, new employees are familiarised with the relevant rules on personal safety and data security. This is done via an awareness training based on Swisscom's electronic learning platform. If the employee fails to participate in this training, he/she shall receive a warning from his/her line manager.

[5] Existing Swisscom employees receive regular training in the careful handling of data. Notifications in the intranet, blog posts, electronic awareness trainings on Swisscom's learning platform and on-site trainings are used for this purpose.

[6] If the Swisscom employee leaves the company, his/her main identity is automatically blocked on Swisscom's systems. The employee's admission to Swisscom's buildings is likewise blocked at the end of his/her last day of work. It is the duty of the employee's supervisor to remove all other accesses and to collect the employee's badge and all Swisscom equipment in the employee's possession on his/her last day of work.

2.8 Availability control

[1] Swisscom stores the data, as contractually agreed, in computer centres that provide the necessary level of protection. These may be computer centres of Swisscom or third parties (see 2.2).

[2] To guarantee the data's availability, Swisscom's storage systems are configured such that the data remain available even if more than one component fails. This is achieved by means of redundant, distributed data carriers, as well as redundant networks and power supplies.

[3] Swisscom secures the data in accordance with the service description. The data are always secured on hard disk systems in an additional computer centre that offers a sufficient geographic distance between the two locations. The different geographical spaces help to reduce potential damage from natural phenomena, such as lightning, rain, flooding and mudslides, as much as possible to one location.

[4] Depending on the services purchased, the Customer can also order different levels of data backups. This is clearly stated in the service description or may be requested from Swisscom's Account Manager.

[5] To harden its systems, Swisscom developed a framework based on the recommendations of the manufacturers, as well as external sources. This framework describes in detail the measures to be implemented for the individual systems. The implementation is inspected regularly and reported centrally. The responsible operating units can call up the results of the inspection at any time and make the necessary corrections based on them. A monthly test report is sent to the relevant operating units.

[6] Swisscom has implemented the necessary processes to identify and evaluate reports of software weaknesses and patches and derive the necessary subsequent steps from this information. The standard patch management process ensures that announcements of system patches are evaluated and installed in the relevant systems following a test. Under certain circumstances, the installation of patches may require the Customer's cooperation and approval. This is taken into account in Swisscom's standardised processes. If a patch must be installed urgently, an emergency patch process applies depending on the service.

2.9 Separation rule

[1] Swisscom ensures that the Customer's data are not reciprocally viewable. To this end, it utilises current security procedures that ensure the separation of customer data at the logical or physical level.

[2] Physical processes are employed when the service and the systems employed for it do not allow for an adequate logical separation. For cost reasons, Swisscom tries to utilise logical processes whenever possible.

[3] Depending on the service offer, the Customer may request, on his/her own initiative, that his/her data be physically separated from those of other customers. This option is not available with all offers.

[4] Swisscom tests its logical processes to ensure that these processes cannot be undermined. Should Swisscom find that the processes no longer guarantee this, Swisscom shall take the necessary countermeasures to re-establish equivalent protection.

2.10 Monitoring, assessment and evaluation

[1] Swisscom performs regular system audits. In the technical unit, this consists of regularly verifying that the basic safeguards are implemented and observed in the systems in accordance with the requirements of Group Security.

[2] New services undergo a technical examination based on a risk analysis. Any defects identified are corrected by the responsible persons at Swisscom. Depending on the severity of the defects, an additional test is carried out to verify that the correction was effective.

[3] In the process area, Swisscom's internal auditing service conducts tests in accordance with a risk-based plan. Tests can also be conducted on an ad-hoc basis anytime by the internal auditing service or at the request of the Board of Directors. The identified defects are corrected within the defined time period and, depending on their severity, re-examined by the internal auditing service.

[4] Group Security operates a risk management system across the entire company to identify and quantify information security

risks and, in conjunction with the responsible organisations, initiate measures to reduce the risks. In the process, Group Security ensures that information security risks are communicated and accounted for at the appropriate levels. Group Security likewise ensure that all relevant risk management officers exchange views about the identified risks and, where practical, establish measures jointly.

5 Group Security runs a bug bounty program for Swisscom. This enables everyone to centrally report identified security gaps in Swisscom's services. The reports are evaluated and the necessary countermeasures taken, e.g. a software patch is created or the code for a website is improved. Finally, the vulnerability report is published by the reporting party, who is compensated based on the severity of the security gap.

6 Group Security has a "Red Team" deployed. The Red Team attacks Swisscom's infrastructures and thus checks the effectiveness of the safeguards implemented. The attacks take place without the Swisscom employees responsible for the systems being aware of it, thereby making it possible to conduct a test under the same conditions that exist when a real attack occurs. The Red Team continues the attacks until a potential access of the data or the target system has been carried out. The attack is then stopped and documented. Data security is guaranteed at all times. By carrying out these operations, Swisscom ensures that the infrastructure is subjected to comprehensive tests. The results are utilised to develop measures that improve the level of security of Swisscom.

7 Swisscom's Data Security Organisation operates a risk management system to identify and document Swisscom's data security risks and to ensure that the identified risks are handled appropriately. In the process, the Data Security Organisation ensures that communication is level-appropriate and that the responsibility for the data security risks is allocated properly. For this purpose, the Data Security Organisation engages in an ongoing exchange with other risk management officers at Swisscom.