Annexe à la convention concernant le traitement des données en sous-traitance

Éléments de données utilisés, mesures techniques et organisationnelles (TOM)

1 Éléments de données utilisés

1.1 Général

Le client met des données personnelles et/ou des données confidentielles à la disposition de Swisscom, à sa seule discrétion et sur son mandat, à des fins de traitement dans le cadre des contrats.

1.2 Personnes concernées

Il peut s'agir de données personnelles, en particulier des personnes concernées suivantes:

- les clients potentiels, les clients, les partenaires commerciaux, les vendeurs et les distributeurs du client - qui sont des personnes physiques
- les employés ou autres auxiliaires des clients potentiels, des clients, des partenaires commerciaux, des vendeurs et des distributeurs
- les employés ou autres auxiliaires du client autorisées par le client à utiliser les services

1.3 Type des données personnel

Il peut s'agir notamment de données personnelles de type suivant:

- les informations personnelles telles que le prénom, le nom, la date de naissance, l'âge, le sexe, la nationalité, etc.
- les coordonnées professionnelles telles que l'adresse électronique, le numéro de téléphone, l'adresse
- les coordonnées privées telles que l'adresse électronique, le numéro de téléphone, l'adresse
- le détail des documents d'identité
- les informations sur la vie professionnelle telles que l'intitulé du poste, la fonction, etc.
- les informations sur la vie privée comme la situation familiale, les passe-temps, etc.
- les informations sur l'utilisateur telles que les données de connexion, le numéro de client, le numéro de personnel, le comportement de l'utilisateur, etc.
- les informations techniques telles que l'adresse IP, les informations sur l'appareil, etc.

1.4 Données personnelles sensibles

Ces catégories de données sont des données personnelles indiquant l'origine raciale ou eth-nique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que des données génétiques et biométriques permettant d'identifier une per-sonne physique de manière unique, les données relatives à la santé ou à la vie sexuelle ou à l'orientation sexuelle.

1.5 Données confidentielles

Il peut s'agir de données relevant, par exemple, du secret professionnel, du secret bancaire, du secret de fonction, du devoir de discrétion en vertu du droit des assurances sociales.

1.6 Délimitations

[1] Si les données ont été cryptées par le client et ne sont donc pas visibles par Swisscom, il ne s'aigt pas de traitement de données en sous-traitance. La convention concernant le traitement des données en sous-traitance n'est pas applicable à ces données.

[2] L'appréciation, si les mesures techniques et organisationnelles décrites ci-dessous pour la protection des données confiées à Swisscom pour leur traitement sont appropriées (notamment pour des données personnelles sensibles ou des données confidentielles), est de la seule responsabilité du client.

[3] Chaque partie traite, dans le cadre de la relation contractuelle, des données personnelles concernant des collaborateurs et autres auxiliaires de l'autre partie. Il s'agit par exemple du nom, de l'adresse postale/e-mail/IP, du numéro de téléphone, de la profession/fonction, des moyens d'identification, des copies de documents d'identité, etc. Aux fins de l'exécution du contrat et du maintien de la relation contractuelle (p. ex. communication, contrôle des accès, annonces de dérangements, commandes, facturations, analyses de satisfaction, informations sur de nouveaux produits, invitations à des événements, etc.), les parties traitent ces données personnelles, en assumant collectivement la responsabilité, sur leurs propres systèmes et en appliquant des mesures techniques et organisationnelles appropriées pour la protection des données. Ce traitement de données n'est pas soumis aux dispositions du traitement de données en sous-traitance, mais Swisscom prend en substance les mesures techniques et organisationnelles décrites ci-dessous.

2 Mesures techniques et organisationnelles

Les chapitres suivants décrivent les mesures prises par Swisscom en matière de protection des données à caractère personnel dans le cadre du traitement des données d'un contrat. Swisscom gère un "Information Security Management System" (ISMS) selon la norme ISO27001:2013. L'ISMS de Swisscom est certifié, le certificat est disponible sur le site Internet de Swisscom (www.swisscom.com/datensicherheit).
Les mesures énumérées ci-dessous doivent être comprises de manière générique et s'appliquent dans chaque cas, sauf indication contraire dans le contrat, par exemple si d'autres mesures spécifiques au produit ou au client sont définies ou si certaines des mesures suivantes sont explicitement exclues. Les mesures suivantes s'appliquent aux cas dans lesquels Swisscom traite elle-même les données pertinentes. Si le traitement des données est effectué par des tiers mandatés par Swisscom, Swisscom veille par des accords contractuels appropriés à ce que les tiers respectent des mesures comparables.

2.1 Contrôle des entrées

[1] Swisscom subdivise les espaces en zones de sécurité avec différents niveaux de sécurité. Ces zones sont subdivisées en zones publiques, zones sécurisées et zones hautement sécurisées. Les zones publiques sont accessibles à tous, telles que les boutiques Swisscom ou les espaces de réception des immeubles de bureaux. Un badge ou une clé est nécessaire pour entrer dans les zones sécurisées. Les badges des employés et des prestataires de services sont personnalisés. La remise de clés aux personnes autorisées est enregistrée. Les visiteurs doivent s'enregistrer et sont accompagnés dans les zones sécurisées par les employés responsables. Si des badges non personnalisés sont utilisés, une personne responsable est désignée pour enregistrer les détenteurs temporaires.

[2] Les centres de données de Swisscom sont classés comme zones hautement sécurisées. Il n'y a pas d'accès direct des zones publiques à la zone de haute sécurité, uniquement un accès par une zone sécurisée. L'entrée dans une zone hautement sécurisée nécessite une identification avec deux éléments et est enregistrée. Les centres de données sont la propriété de Swisscom ou sont loués pour des périodes de longue durée à des tiers.

[3] Les centres de données de Swisscom disposent des mesures de protection physique nécessaires pour détecter rapidement une violation du périmètre du bâtiment et déclencher une alarme correspondante. Pour les bâtiments qui sont occupés 24 heures sur 24, le personnel de sécurité est formé pour traiter ces alarmes rapidement et professionnellement et prendre les mesures appropriées. Si les bâtiments ne sont pas occupés 24 heures sur 24, les alarmes sont transmises à un service de sécurité ou à la police pour déclencher une intervention.

[4] Les centres de données de Swisscom disposent de toutes les mesures de protection nécessaires pour réduire autant que possible les risques de phénomènes naturels tels que la foudre, la pluie, les inondations, etc., de telle sorte qu'ils n'ont plus d'incidence sur le fonctionnement des centres de données.

[5] Si Swisscom fait appel à des centres de données tiers pour le stockage permanent de données destinées aux services de Swisscom, Swisscom s'assure que les exploitants de ces centres de données remplissent des conditions comparables à celles des centres de données de Swisscom et assurent ainsi un niveau de sécurité équivalent.

[6] Dans le cas où le client stocke ses données sur place chez lui, Swisscom peut formuler des recommandations sur la façon de sécuriser ces locaux. Il relève de la responsabilité du client de prendre les mesures de protection nécessaires.

2.2 Contrôle des accès au système

[1] L'accès aux systèmes de Swisscom s'effectue toujours avec les identifiants personnalisés des personnes mandatées par Swisscom.

[2] L'accès aux systèmes est toujours protégé par au moins un mot de passe ou un élément d'authentification équivalent et l'identification numérique associée. Les données d'accès sont stockées de sorte qu'aucune déduction directe de l'élément d'authentification valide ne soit possible si ces données deviennent accessibles.

[3] Les mots de passe doivent répondre à des exigences complexes et se composer d'au moins trois classes des éléments suivants: lettres majuscules, lettres minuscules, chiffres, caractères spéciaux. Les mots de passe des comptes personnels ne seront jamais mis à la disposition de tiers.

[4] En cas de connexion incorrecte, l'identification est d'abord temporairement bloquée puis définitivement après d'autres tentatives infructueuses. Le déblocage n'est alors possible qu'avec l'aide du Service Desk de Swisscom. Mobile ID est utilisé pour identifier l'utilisateur.

[5] Si l'utilisateur a besoin de droits d'administrateur avec une identité impersonnelle, l'utilisateur doit effectuer une procédure de «Step-up»: cela signifie que l'employé se connecte au système avec son compte personnel, puis augmente ses droits sur le système. Sur les systèmes Unix, par exemple, cela s'effectue en utilisant la commande sudo. Si aucune procédure de «Step-up» n'est possible, Swisscom peut déterminer à tout moment par l'intermédiaire de la plate-forme d'administration quel utilisateur a utilisé l'identité d'administrateur impersonnelle. Tous les accès administratifs sont enregistrés de manière centralisée chez Swisscom et stockés pendant une durée déterminée.

[6] Pour accéder aux portails accessibles par Internet, les utilisateurs doivent fournir, en fonction de leur classification, une authentification forte en cas d'accès aux données pertinentes. L'authentification forte est basée sur Mobile ID, l'utilisation d'un jeton électronique pour générer des mots de passe à usage unique ou d'autres moyens sécurisés en tant que second élément.

[7] Mobile ID est un service de Swisscom basé sur une carte SIM spécifiquement adaptée à Swisscom avec un module de sécurité pour téléphones mobiles, constituant ainsi une identification sécurisée de l'utilisateur.

[8] Les appareils qui accèdent directement au réseau de l'entreprise sont identifiés par un certificat. Les employés qui utilisent leur appareil personnel doivent se connecter par une infrastructure virtuelle pour accéder aux données client pertinentes.

2.3 Contrôle des accès aux données

[1] Les autorisations sur les systèmes sont structurées en rôles. Une identité se voit attribuer un ou plusieurs rôles nécessaires à l'exécution du rôle organisationnel de la personne. Les rôles sont structurés de sorte que seules les données nécessaires pour accomplir la tâche peuvent être accessibles.

[2] La description des rôles et de leurs autorisations est documentée dans le concept des rôles. Ce concept est régulièrement revu et mis à jour. Le concept de rôle est géré et mis à jour par le responsable du système. Pour tous les rôles, une vérification régulière est effectuée pour savoir si les utilisateurs affectés ont toujours besoin de ce rôle.

[3] Si un employé a besoin de droits supplémentaires, il peut commander un rôle supplémentaire. Ce rôle supplémentaire est autorisé par le supérieur et le titulaire du rôle. Le titulaire du rôle peut décider si cette autorisation est réellement nécessaire ou si une autorisation automatique peut avoir lieu. Un nombre très limité de rôles sont automatiquement attribués à l'employé, il s'agit de rôles de la structure organisationnelle, tels que l'appartenance à une unité organisationnelle.

[4] L'accès avec des droits accrus pour administrer les systèmes de Swisscom se fait toujours par l'intermédiaire d'une infrastructure dédiée avec authentification forte. Toutes les connections, les déconnections et les connections incorrectes sont enregistrées de manière centralisée et stockées pendant une durée déterminée. L'authentification forte est basée sur Mobile ID ou sur l'utilisation d'un jeton électronique pour générer des mots de passe à usage unique.

[5] Le flux de données entre le réseau du client et Swisscom est si possible crypté ou protégé par des mesures alternatives. Les mesures alternatives peuvent être, par exemple, l'utilisation de lignes logiques dédiées ou l'utilisation de connexions directes par fibre optique. Le cryptage de la connexion est basé sur des protocoles et des mécanismes de protection actuels.

[6] Les accès aux systèmes sont enregistrés de manière centralisée et analysés par diverses procédures et font l'objet d'une vérification en cas de violation de la sécurité de l'information. Les violations identifiées sont analysées par une équipe centrale et les mesures appropriées sont prises.

2.4 Contrôle de la transmission

[1] L'accès aux données pertinentes par Internet se fait toujours par une connexion cryptée. Swisscom utilise des protocoles et des mécanismes de protection actuels. Cette connexion cryptée est basée sur des technologies de réseau, des couches de session ou d'application.

[2] L'accès direct du client à ses données à caractère personnel est protégé en accord avec le client par la transmission. Swisscom propose à cet égard des services appropriés qui permettent au client de se connecter à un réseau virtuel. En outre, d'autres techniques de cryptage peuvent également être utilisées pour ces connexions.

[3] Afin de prévenir la fuite de données, Swisscom a mis en place des mesures de protection pour les interfaces entre le courrier électronique et le Web, qui vérifient si des données à caractère personnel sont transmises en grande quantité et constituent donc une fuite possible de ces données vers Internet.

2.5 Contrôle du stockage

[1] Le stockage permanent dans les centres de données est protégé contre les pertes par des mesures de protection physique. Celles-ci comprennent des alimentations électriques redondantes et les systèmes nécessaires pour permettre un fonctionnement autonome pendant une durée limitée.

[2] Les pièces hautement sécurisées sont équipées de systèmes d'alarme incendie et de détection de fumée. En cas d'inci-

dent, soit le personnel de sécurité ou le personnel du bâtiment présent sera déployé pour une première réaction, soit un système d'extinction sera activé afin de minimiser le plus possible les dommages potentiels. S'il n'y a pas de personnel sur le site, l'alarme sera transmise aux pompiers locaux.

3 En cas de défaut, Swisscom rend les supports de données physiquement inutilisables afin d'exclure complètement tout accès éventuel.

4 Les supports de données fonctionnels sont supprimés en utilisant des techniques de suppression standard dans la branche, ce qui rend presque impossible la reconstitution des données qu'ils contiennent. Si une telle procédure n'est pas possible, les supports de données sont physiquement rendus inutilisables, c'est-à-dire détruits.

5 Une restitution des supports de données au client est possible dans des circonstances définies. Cela suppose que le système de stockage, respectivement le support de données n'a été utilisé que pour ce client. Dans ce cas, Swisscom dispose d'une procédure définie pour enregistrer la remise au client des supports de données dans un bâtiment de Swisscom.

2.6 Contrôle des saisies

1 Dans le cas où Swisscom est responsable de la saisie et du traitement de données à caractère personnel, Swisscom s'assure, avec les mesures techniques et organisationnelles nécessaires, que ces données sont correctement collectées et traitées. Des mesures techniques sont utilisées pour vérifier la validité des données, par exemple il est vérifié si une référence à la personne existe déjà dans un autre système pertinent. Les mesures organisationnelles pour vérifier l'exactitude sont, par exemple, un contrôle ultérieur des saisies et des ajustements ou un contrôle aléatoire de l'exactitude des données.

2 Swisscom collecte d'autres données à caractère personnel du client dans les systèmes Swisscom en vue de la fourniture du service. Ces systèmes sont utilisés, par exemple, pour collecter les messages d'erreur (incidents), les demandes de modification ou la facturation. Swisscom s'assure, par des mesures de qualité appropriées, que les données pertinentes collectées dans ce cadre sont vérifiées et corrigées.

2.7 Contrôle des mandats

1 Swisscom sélectionne avec soin les éventuels sous-traitants ayant accès aux données et transfère les responsabilités pertinentes relatives à la protection des données au fournisseur.

2 Swisscom a désigné une organisation responsable pour garantir les exigences en matière de protection des données. Celle-ci est atteignable pour toute demande de renseignement sous datenschutz@swisscom.com. Le premier interlocuteur pour les questions relatives à la protection des données chez Swisscom est l' account manager de Swisscom.

3 Les nouveaux employés de Swisscom sont soumis à un contrôle de sécurité avant leur entrée en fonction. Il se compose de différentes étapes et est conçu différemment en fonction des possibilités d'accès aux données pertinentes. Le contrôle comprend au moins la vérification du curriculum vitae complet, des derniers certificats et l'obtention des références personnelles.
Les autres étapes comprennent également la signature d'une déclaration de confidentialité ainsi que l'examen d'un extrait actuel du casier judiciaire et d'un extrait actuel du registre des poursuites.

4 Les nouveaux employés sont familiarisés avec les règles pertinentes relatives à leur propre sécurité et à la sécurité des données au début de leur fonction. La familiarisation se fait par un Awareness Training basé sur la plate-forme d'apprentissage électronique de Swisscom. En cas de non-participation, une relance est effectuée par le supérieur hiérarchique de l'employé.

5 Les employés actuels de Swisscom reçoivent une formation régulière sur le traitement rigoureux des données. Elle englobe des messages sur Intranet, des articles de blog, des formations à la sensibilisation électronique sur la plate-forme d'apprentissage de Swisscom ainsi que des formations sur place.

6 Lorsque l'employé de Swisscom quitte l'entreprise, l'identité principale est automatiquement bloquée sur les systèmes de Swisscom. L'accès aux bâtiments est également bloqué à la fin du dernier jour de travail. Il appartient au supérieur de supprimer tous les autres accès et de récupérer le badge et les outils de travail de Swisscom le dernier jour de travail de l'employé.

2.8 Contrôle de la disponibilité

1 Swisscom stocke les données dans les centres de données avec le niveau de protection nécessaire, comme convenu contractuellement. Il peut s'agir de centres de données exploités par Swisscom ou par des tiers (voir 2.2).

2 Pour garantir la disponibilité des données, les systèmes de stockage de Swisscom sont configurés de manière à ce que plusieurs composants puissent tomber en panne et que les données soient toujours disponibles. Ceci est possible grâce à des supports de données redondants et répartis ainsi que par des réseaux et des alimentations électriques redondants.

3 Swisscom sauvegarde les données conformément à la description du service. La sauvegarde est toujours effectuée sur des systèmes de disque dur dans un autre centre de données avec une distance géographique suffisante entre les deux endroits. Les différentes zones géographiques servent à réduire le plus possible les dommages éventuels causés par des phénomènes naturels tels que la foudre, la pluie, les inondations, les coulées de débris à un seul endroit.

4 Suivant les services achetés, le client peut en outre commander différents niveaux de sauvegardes de données. Ceci est indiqué dans la description du service ou peut être demandé auprès de l'account manager de Swisscom.

5 Swisscom a développé un cadre pour consolider les systèmes sur la base des recommandations des fabricants et de sources externes. Ce cadre décrit en détail les mesures à mettre en œuvre pour chaque système. La mise en œuvre fait l'objet de contrôles réguliers et de rapports centralisés. Les unités opérationnelles responsables peuvent consulter à tout moment les résultats du contrôle et sur cette base apporter les corrections nécessaires. Un rapport de contrôle mensuel est envoyé aux unités opérationnelles concernées.

6 Swisscom a mis en œuvre les processus nécessaires pour identifier et évaluer les messages relatifs aux vulnérabilités des logiciels et aux patches et pour en déduire les étapes ultérieures nécessaires. Le processus standard de Patch Management garantit que les notifications de patches aux systèmes sont évaluées et installées sur les systèmes concernés après un contrôle. Selon les circonstances, l'installation de patches peut nécessiter la collaboration et l'autorisation du client. Cela est pris en compte dans les processus standardisés de Swisscom. Il existe un processus de patch d'urgence pour chaque service si un patch doit être installé d'urgence.

2.9 Principe de séparation

1 Swisscom s'assure que les données des clients ne sont pas visibles mutuellement. À cet effet, les procédures de sécurité en vigueur sont utilisées pour assurer la séparation des données client à un niveau logique ou physique.

2 Les procédures physiques sont mises en place lorsque le service et les systèmes associés utilisés ne permettent pas une séparation logique adéquate. Pour des raisons de coûts, Swisscom essaie toujours d'utiliser des procédures logiques.

3 En fonction de l'offre de service, le client peut exprimer le souhait que ses données soient physiquement séparées des

données d'autres clients. Cette option n'est pas disponible dans toutes les offres.

4 Les procédures logiques ont été vérifiées par Swisscom pour s'assurer que ces procédures ne puissent pas être contournées. Si Swisscom constate que les procédures n'offrent plus une garantie suffisante, Swisscom prendra les contre-mesures nécessaires pour rétablir une protection équivalente.

2.10 Contrôle, analyse et évaluation

1 Swisscom effectue régulièrement des audits des systèmes. Au niveau technique, il s'agit d'un contrôle régulier de la mise en œuvre et du respect des mesures de protection de base sur les systèmes, conformément aux exigences du Groupe Security.

2 Sur la base d'une analyse des risques, les nouveaux services et prestations font l'objet d'un examen technique. Les défauts identifiés sont corrigés par les responsables de Swisscom. En fonction de la gravité des défauts, un contrôle supplémentaire sera effectué pour établir l'efficacité de la correction.

3 Dans le domaine des processus, le service d'audit interne effectue des contrôles en fonction d'une planification basée sur les risques. Des contrôles peuvent également être effectués de manière ad hoc à tout moment par le service d'audit interne ou à la demande du Conseil d'administration de Swisscom. Les défauts identifiés seront corrigés dans les délais impartis et, en fonction de la gravité, ils seront à nouveau contrôlés par le service d'audit interne.

4 Le Group Security gère un système de gestion des risques dans l'ensemble de l'entreprise pour identifier et quantifier les risques de sécurité de l'information et prendre des mesures pour réduire les risques avec les organisations responsables. Le Group Security garantit que les risques liés à la sécurité de l'information sont communiqués et gérés par les responsables. Le Group Security s'assure également que toutes les fonctions pertinentes de gestion des risques échangent des informations sur les risques identifiés et, le cas échéant, déterminent conjointement les mesures à prendre.

5 Le Group Security est responsable du programme Bug Bounty pour Swisscom. Cela permet à quiconque de signaler de manière centralisée les failles de sécurité détectées dans les services de Swisscom. Les signalements sont évalués et les contre-mesures nécessaires sont prises, par exemple la création d'un patch pour un logiciel ou l'amélioration du code d'une page Web. Enfin, le signalement de vulnérabilité est publié par l'auteur du signalement qui est dédommagé en fonction de la gravité de la faille.

6 Le Group Security dispose d'une "Red team". La "Red Team" attaque les infrastructures de Swisscom, vérifiant ainsi l'efficacité des mesures de sécurité prises. Les attaques sont effectuées à l'insu des employés de Swisscom responsables des systèmes et permettent ainsi un contrôle dans les mêmes conditions que dans le cas d'une attaque réelle. Les attaques continuent jusqu'à ce que l'accès aux données ou au système cible soit possible. L'attaque est ensuite arrêtée et documentée. La sécurité des données est garantie à tout moment. À l'aide de ces opérations, Swisscom garantit des tests d'infrastructure complets. Des mesures sont déduites des résultats en vue d'améliorer le niveau de sécurité de Swisscom.

7 L'organisation de la protection des données de Swisscom gère un système de gestion des risques afin d'identifier et de documenter les risques liés à la protection des données de Swisscom et d'assurer un traitement approprié des risques identifiés. L'organisation de la protection des données garantit la communication aux responsables et la répartition des responsabilités en matière de risques relatifs à la protection des données. L'organisation de la protection des données est en contact permanent avec les autres fonctions de gestion des risques de Swisscom.