Éléments de données utilisés et mesures techniques et organisationnelles (MTO)

1 Éléments de données utilisés

1.1 Généralités

Dans le cadre des contrats, le client confie à Swisscom Broadcast SA, ci-après «Swisscom», à sa propre discrétion et sur mandat du client, des données personnelles et/ou tenues au secret à des fins de traitement.

1.2 Personnes concernées

Il peut s'agir de données personnelles, concernant en particulier les personnes suivantes:

- prospects, clients, partenaires commerciaux, vendeurs et distributeurs du client – qui sont des personnes physiques,
- collaborateurs ou autres auxiliaires des prospects, clients, partenaires commerciaux, vendeurs et distributeurs,
- collaborateurs ou autres auxiliaires du client qui ont été autorisés par le client à utiliser les services.

1.3 Nature des données personnelles

Il peut s'agir en particulier des types de données personnelles suivants:

- informations personnelles telles que le prénom, le nom de famille, la date de naissance, l'âge, le sexe, la nationalité, etc.,
- coordonnées professionnelles telles que l'adresse e-mail, le numéro de téléphone, l'adresse postale,
- coordonnées privées telles que l'adresse e-mail, le numéro de téléphone, l'adresse postale,
- détails des papiers d'identité,
- informations sur la vie professionnelle telles que l'intitulé du poste, la fonction, etc.,
- informations sur la vie privée telles que la situation familiale, les loisirs, etc.,
- informations sur l'utilisateur telles que les données de connexion, le numéro de client, le numéro personnel, les habitudes d'utilisation, etc.,
- informations techniques telles que l'adresse IP, les informations sur l'appareil, etc.,

1.4 Données personnelles sensibles

Ces catégories de données concernent des données personnelles sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques et biométriques permettant d'identifier une personne physique de manière univoque, des données de santé ou en lien avec la vie sexuelle ou l'orientation sexuelle.

1.5 Données à caractère secret

Il peut s'agir entre autres de données soumises au secret professionnel, au secret bancaire, au secret de fonction, au devoir de discrétion selon le droit des assurances sociales.

2 Mesures techniques et organisationnelles

2.1 Généralités

1 Les chapitres suivants décrivent les mesures techniques et organisationnelles prises par Swisscom concernant la protection des données personnelles dans le cadre de la sous-traitance du traitement desdites données. Il incombe exclusivement au client d'évaluer si les mesures décrites ci-après sont adaptées à la protection des données confiées à Swisscom en vue de leur traitement (notamment pour les données personnelles sensibles ou celles tenues au secret).

2 Swisscom gère un Information Security Management System (ISMS), basé sur la norme ISO 27001 et d'autres normes internationales.

3 Les mesures mentionnées ci-après sont à comprendre de manière générique et s'appliquent sauf disposition contraire dans le contrat, p. ex. si des mesures plus détaillées spécifiques au produit ou au client sont définies ou si certaines des mesures ci-après sont explicitement exclues. Les mesures suivantes s'appliquent dans tous les cas où Swisscom traite elle-même les données pertinentes. Si ledit traitement est assuré par des tiers mandatés par Swisscom, cette dernière veille, via des accords contractuels appropriés, à ce que lesdits tiers respectent des mesures comparables.

2.2 Contrôle des entrées

1 Swisscom subdivise les espaces en zones de sécurité dotées de différents niveaux de protection. Les zones sont réparties en zones publiques, sécurisées ou hautement sécurisées. Les zones publiques sont accessibles à tout le monde, p. ex. les espaces de réception dans un immeuble de bureaux. Un badge ou une clé est requis pour pénétrer des zones sécurisées. Les badges du personnel et des prestataires sont individuels. La remise des clés aux personnes autorisées est consignée. Les visiteurs doivent s'enregistrer et être accompagnés par des responsables dans les zones sécurisées. En cas d'utilisation de badges non personnalisés, un responsable est désigné et tient un journal des détenteurs temporaires.

2 Les centres de calcul Swisscom sont classés comme zones hautement sécurisées. Il n'est pas possible d'accéder directement d'une zone publique à une zone hautement sécurisée, il est nécessaire de passer par une zone sécurisée. Pour pénétrer une zone hautement sécurisée, une identification à l'aide de deux éléments est requise, et elle fait l'objet d'un protocole. Les centres de calcul sont la propriété de Swisscom ou bien sont loués à des tiers pour des périodes de longue durée.

3 Les centres de calcul Swisscom disposent des mesures de protection physiques nécessaires pour détecter aussitôt une violation du périmètre du bâtiment et déclencher une alarme correspondante. Dans les bâtiments occupés 24 h/24, le personnel de sécurité est formé en conséquence pour traiter de façon rapide et professionnelle lesdites alertes et prendre les mesures qui s'imposent. Pour les autres bâtiments, les alarmes sont transmises à un prestataire de sécurité ou à la police afin d'initier une intervention.

4 Les centres de calcul Swisscom disposent des autres mesures de protection nécessaires pour réduire autant que possible les risques liés aux phénomènes naturels, tels que la foudre, la pluie, les inondations, etc., afin d'éliminer leur pertinence pour l'exploitation du centre de calcul.

5 Si, pour les prestations de Swisscom, des centres de calcul de tiers sont utilisés pour stocker des données en permanence, Swisscom s'assure que les exploitants dudit centre remplissent des conditions comparables à celles des centres de calcul Swisscom et donc appliquent un niveau de sécurité équivalent.

6 Au cas où le client stocke ses données sur son propre site, Swisscom peut émettre des recommandations sur la manière de sécuriser les locaux en question. Il revient au client de prendre les mesures de protection nécessaires.

2.3 Contrôle des accès

1 L'accès aux systèmes de Swisscom requiert toujours l'identification individuelle des personnes mandatées par Swisscom.

2 La protection s'effectue toujours par au moins un mot de passe ou une authentification équivalente ainsi que par l'identification numérique correspondante. Les données d'accès sont sauvegardées de façon à empêcher tout lien direct avec l'authentification valable, au cas où ces données deviendraient accessibles.

3 Les mots de passe doivent répondre à des exigences complexes et se composer d'au minimum trois catégories parmi les éléments suivants: majuscules, minuscules, chiffres, caractères spéciaux. Les mots de passe de comptes personnels ne sont jamais rendus accessibles à des tiers.

4 En cas d'erreur de connexion, l'identification peut être bloquée, d'abord temporairement, puis définitivement après de nouvelles tentatives infructueuses.

5 Les portails accessibles via Internet exigent, selon la classification des utilisateurs, une authentification forte pour consulter les données pertinentes. L'authentification forte est basée sur le Mobile ID, l'utilisation d'un jeton électronique pour générer des mots de passe à usage unique ou d'autres moyens sécurisés comme deuxième facteur.

2.4 Autorisations d'accès

1 Les autorisations dans les systèmes sont structurées en rôles. Une identité se voit attribuer un ou plusieurs rôles qui sont nécessaires pour exécuter le rôle organisationnel de la personne. Les rôles sont organisés de manière à ce que seules les données nécessaires à l'exécution de la mission puissent être accessibles. La description des rôles et leurs autorisations sont documentées dans des concepts de rôles.

2 Si un collaborateur a besoin de droits complémentaires, il peut commander un rôle supplémentaire. Ledit rôle supplémentaire est validé par le supérieur et le titulaire du rôle. Le titulaire du rôle peut décider si cette validation est effectivement nécessaire ou si une validation automatique est possible. Un nombre très limité de rôles sont attribués automatiquement au collaborateur. Cela concerne ceux issus de la structure organisationnelle, p. ex. l'appartenance à une unité d'organisation.

3 Dans la mesure du possible, le trafic de données entre le réseau du client et Swisscom est crypté ou protégé par des mesures alternatives. Les mesures alternatives peuvent consister à utiliser des lignes logiques dédiées ou bien des liaisons directes en fibre optique. Le cryptage de la connexion repose sur des protocoles et des mécanismes de protection actuels.

4 Les accès aux systèmes sont consignés et peuvent être analysés par différents procédés.

2.5 Contrôle du transport

1 L'accès aux données pertinentes via Internet requiert toujours une connexion cryptée. À cet effet, Swisscom utilise des protocoles et des mécanismes de protection actuels. La connexion cryptée repose sur des technologies au niveau du réseau, de la session ou de la couche applicative.

2 L'accès direct du client à ses données personnelles est protégé par le moyen de transport, après accord avec le client. Swisscom propose dans ce cas des services appropriés, qui permettent des connexions réseau virtuelles avec le client. De plus, d'autres techniques de cryptage peuvent être utilisées pour ces connexions.

2.6 Contrôle de la mémoire

1 Les mémoires permanentes dans les centres de calcul sont protégées contre les pertes par des mesures de protection physiques. Cela inclut notamment des alimentations électriques redondantes et les systèmes nécessaires pour permettre un fonctionnement autonome pendant une période définie.

2 Pour se protéger contre les dommages causés par la fumée ou le feu, les locaux hautement sécurisés sont dotés de systèmes de détection appropriés. En cas d'incident, le personnel de sécurité ou le personnel du bâtiment présent intervient pour une première réaction, ou bien un système d'extinction se déclenche pour réduire au maximum les dommages potentiels. En l'absence de personnel sur place, l'alarme est transmise aux pompiers locaux.

3 Si des supports de données deviennent défectueux, ils sont rendus physiquement inutilisables par Swisscom afin d'exclure tout accès.

4 Les supports de données opérationnels sont effacés via les procédures usuelles dans le secteur, de sorte qu'il soit pratiquement impossible de reconstituer les données contenues. Dans l'incapacité d'appliquer une telle procédure, les supports de données sont rendus physiquement inutilisables, voire détruits.

5 Les supports de données peuvent être restitués au client dans les conditions définies. Cela suppose que le système d'archivage ou le support de données n'ait été utilisé que pour ce seul client.

2.7 Contrôle des saisies

1 Lorsque Swisscom est responsable de la saisie et du traitement de données personnelles, elle prend les mesures nécessaires pour s'assurer que lesdites données sont correctement saisies et traitées.

2 Pour la fourniture de services, Swisscom saisit d'autres données personnelles du client dans des systèmes de Swisscom. Ces systèmes servent par exemple à enregistrer des messages d'erreur (incidents), saisir des demandes de modification ou établir la facturation. Swisscom s'assure, par des mesures de qualité appropriées, que les données pertinentes saisies à cette occasion sont vérifiées et corrigées.

2.8 Contrôle de la sous-traitance

1 Swisscom sélectionne avec soin les potentiels sous-traitants ayant accès aux données et confie aux fournisseurs les responsabilités pertinentes en matière de protection des données.

2 Swisscom a désigné une organisation responsable pour garantir les exigences de protection des données. Cette dernière est joignable pour toute demande à l'adresse datenschutz.sbc@swisscom.com. Le premier interlocuteur Swisscom pour les questions sur la protection des données est l'Account Manager compétent de Swisscom.

3 Les nouvelles recrues de Swisscom sont soumises à un contrôle de sécurité avant le début de leur engagement. Ce dernier comprend plusieurs niveaux et varie selon les possibilités d'accès aux données pertinentes. Le contrôle inclut au minimum la vérification du curriculum vitae complet, des derniers certificats et l'obtention d'une référence personnelle.
Les étapes suivantes prévoient la signature d'une déclaration de confidentialité ou une vérification selon le contrôle de sécurité relatif aux personnes de la Confédération.

4 Lors de leur entrée en fonction, les nouvelles recrues sont initiées aux règles pertinentes concernant leur propre sécurité et celle des données.

5 Les collaborateurs actuels de Swisscom sont régulièrement formés au bon usage des données. À cet effet sont prévus des messages sur l'Intranet, des articles de blog, des formations électroniques de sensibilisation sur la plateforme d'apprentissage de Swisscom ainsi que des formations sur site.

6 Au départ de l'entreprise, l'identité principale du collaborateur Swisscom concerné est automatiquement bloquée dans les systèmes de Swisscom. L'accès aux bâtiments est également bloqué à la fin du dernier jour de travail. Il incombe au supérieur de supprimer tous les autres accès et de reprendre le badge et les outils de travail Swisscom le dernier jour de travail du collaborateur.

2.9 Contrôle de disponibilité

1 Conformément à l'accord contractuel, Swisscom stocke les données dans des centres de calcul offrant le niveau de protection requis. Il peut s'agir de centres de calcul Swisscom ou de tiers.

2 Afin de garantir la disponibilité des données, les systèmes d'archivage de Swisscom sont configurés de façon à maintenir la disponibilité des données malgré plus d'un composant en panne. Cette solution est rendue possible par 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 de service. La sauvegarde peut avoir lieu sur des systèmes d'archivage dans un autre centre de calcul, avec une distance géographique suffisante entre les deux sites. La séparation géographique permet de minimiser si possible sur un seul site les éventuels dommages causés par des phénomènes naturels, tels que la foudre, la pluie, les inondations, les coulées de boue.

4 Selon les prestations souscrites, le client peut en plus commander différents niveaux de sauvegarde de données. Ce point figure dans la description du service ou peut être demandé à l'Account Manager de Swisscom.

5 Swisscom a mis en place les processus nécessaires pour identifier et analyser les messages relatifs à des failles logicielles et des correctifs et pour en déduire les mesures à prendre.

2.10 Principe de séparation

1 Swisscom s'assure que les données des clients ne peuvent pas être consultées mutuellement. À cet effet, elle applique des procédures de sécurité actuelles qui garantissent la séparation des données clients au niveau logique ou physique.

2 Les procédures physiques sont appropriées lorsque le service et les systèmes associés utilisés ne permettent pas d'assurer une séparation logique adéquate. Pour des raisons de coûts, Swisscom s'évertue dans la mesure du possible à toujours utiliser des procédures logiques.

3 Selon l'offre de service, le client peut exprimer le souhait que ses données soient physiquement séparées de celles des autres clients. Cette option n'est pas disponible dans toutes les offres.

4 Les procédures logiques ont été contrôlées par Swisscom afin de s'assurer qu'elles ne peuvent pas être neutralisées. Si Swisscom constate que lesdites procédures ne garantissent plus la protection requise, elle prendra les contre-mesures nécessaires pour rétablir une protection équivalente.

2.11 Contrôle, analyse et évaluation

1 Swisscom procède à des audits réguliers des systèmes. Au niveau technique, il peut s'agir d'un contrôle régulier du périmètre IP ou d'audits de sécurité sur les plateformes.

2 À partir d'une analyse des risques, de nouvelles prestations et de nouveaux services sont soumis à un contrôle technique. Les défauts constatés sont corrigés par les services compétents. Selon la gravité desdits défauts, un examen complémentaire est réalisé afin de prouver la bonne correction.

3 Swisscom exploite un système de gestion des risques dans toute l'entreprise afin de déterminer et de quantifier les risques et d'instaurer des mesures de réduction des risques en collaboration avec les organisations responsables.

4 Swisscom participe à un programme Bug Bounty. Ce dernier permet à toute personne d'annoncer de manière centralisée les failles de sécurité identifiées dans les services Swisscom. Les avis sont analysés et les contre-mesures nécessaires sont prises, p. ex. l'élaboration d'un patch pour un logiciel ou l'amélioration du code sur une page web.