Anhang zur Vereinbarung über die Auftragsdatenbearbeitung

Verwendete Datenelemente und technische und organisatorische Massnahmen (TOM)

1 Verwendete Datenelemente

1.1 Generell

Der Kunde überlässt Swisscom Broadcast AG nachfolgend "Swisscom" genannt im Rahmen der Verträge in seinem eigenen Ermessen und in seinem Auftrag Personendaten und/oder geheimnisgebundene Daten zur Bearbeitung.

1.2 Betroffene Personen

Es kann sich dabei um Personendaten insbesondere folgender betroffener Personen handeln:

- Potentielle Kunden, Kunden, Geschäftspartner, Verkäufer und Händler des Kunden – welche natürliche Personen sind
- Mitarbeitende oder andere Hilfspersonen von potentiellen Kunden, Kunden, Geschäftspartnern, Verkäufern und Händlern
- Mitarbeitende oder andere Hilfspersonen des Kunden, welche durch den Kunden berechtigt wurden die Services zu nutzen

1.3 Art von Personendaten

Es kann sich dabei insbesondere um folgende Arten von Personendaten handeln:

- Persönliche Informationen wie Vorname, Nachname, Geburtsdatum, Alter, Geschlecht, Nationalität etc.
- Geschäftliche Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse
- Private Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse
- Details von Identitätspapieren
- Informationen über das Berufsleben wie Stellenbezeichnung, Funktion etc.
- Informationen über das private Leben wie Familienstand, Hobbies etc.
- Benutzerinformationen wie Logindaten, Kundennummer, Personalnummer, Nutzerverhalten etc.
- Technische Informationen wie IP-Adresse, Geräteinformationen etc.

1.4 Besonders schützenswerte Personendaten

Bei diesen Datenkategorien handelt es sich um Personendaten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

1.5 Geheimnisgebundene Daten

Bei diesen Daten kann es sich beispielsweise um dem Berufsgeheimnis, dem Bankgeheimnis, dem Amtsgeheimnis, der Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegende Daten handeln.

2 Technische und organisatorische Massnahmen

2.1 Generelles

[1] Die folgenden Kapitel beschreiben die von Swisscom getroffenen technischen und organisatorischen Massnahmen in Bezug auf den Schutz von Personendaten im Rahmen der Auftragsdatenbearbeitung. Die Beurteilung, ob die nachfolgend beschriebenen Massnahmen zum Schutz der Swisscom zur Bearbeitung anvertrauten Daten (namentlich bei besonders schützenswerten Personendaten oder geheimnisgebundenen Daten) angemessen sind, obliegt ausschliesslich dem Kunden.

[2] Swisscom unterhält ein Information Security Management System (ISMS), welches sich an ISO27001 und andere internationale Standards anlehnt.

[3] Die nachstehend aufgeführten Massnahmen sind generisch zu verstehen und kommen jeweils dann zur Anwendung, wenn im Vertrag nichts Abweichendes definiert ist, z.B. weitergehende produkt- oder kundenspezifische Massnahmen festgelegt sind oder gewisse der nachstehenden Massnahmen explizit ausgeschlossen werden. Die nachfolgenden Massnahmen gelten für die Fälle, in welchen Swisscom selbst die relevanten Daten verarbeitet. Findet die Datenbearbeitung durch von Swisscom beauftragte Dritte statt, sorgt Swisscom mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Dritten vergleichbare Massnahmen einhalten.

2.2 Zutrittskontrolle

[1] Swisscom unterteilt die Flächen in verschieden stark gesicherte Sicherheitszonen. Diese Zonen unterteilen sich in öffentliche, gesicherte und hochsichere Zonen. Öffentliche Zonen sind für jedermann zugänglich, wie z.B. die Empfangsräumlichkeiten in einem Bürogebäude. Um in gesicherte Zonen Zutritt zu erhalten, wird ein Badge oder Schlüssel benötigt. Die Badges der Mitarbeitenden und Dienstleister sind personalisiert. Die Ausgabe der Schlüssel an die berechtigten Personen wird protokolliert. Besucher müssen sich registrieren und werden in den gesicherten Zonen von den verantwortlichen Mitarbeitenden begleitet. Sind nicht personalisierte Badges im Einsatz, ist ein Verantwortlicher benannt, der über die temporären Besitzer ein Protokoll führt.

[2] Rechenzentren von Swisscom sind als hochsichere Zonen klassifiziert. Es gibt keinen direkten Zugang von öffentlichen Zonen zur hochsicheren Zone, sondern nur über eine gesicherte Zone. Der Zutritt zur hochsicheren Zone verlangt eine Identifikation mit zwei Elementen, und wird protokolliert. Die Rechenzentren sind im Eigentum von Swisscom, oder für langfristige Zeiträume von Dritten gemietet.

[3] Rechenzentren von Swisscom verfügen über die nötigen physischen Schutzmassnahmen, um eine Verletzung des Perimeters des Gebäudes frühzeitig zu erkennen und einen entsprechenden Alarm auszulösen. Bei Gebäuden, die rund um die Uhr besetzt sind, sind die Sicherheitsmitarbeitenden entsprechend geschult, um solche Alarmierungen rasch und professionell zu verarbeiten und entsprechende Massnahmen einzuleiten. Falls die Gebäude nicht rund um die Uhr besetzt sind, gehen die Alarme an einen Sicherheitsdienstleister oder an die Polizei um eine Intervention auszulösen.

[4] Rechenzentren von Swisscom verfügen über die weiteren nötigen Schutzmassnahmen um Gefahren durch Naturereignisse wie Blitz, Regen, Überschwemmung etc. möglichst so stark zu reduzieren, dass diese nicht mehr relevant für den Rechenzentrumsbetrieb sind.

[5] Falls für Dienstleistungen von Swisscom Rechenzentren von Dritten für die permanente Speicherung von Daten genutzt werden, stellt Swisscom sicher, dass die Betreiber eines solchen Rechenzentrums vergleichbare Bedingungen wie die Rechenzentren von Swisscom und damit ein äquivalentes Sicherheitsniveau erfüllen.

[6] Im Falle, dass der Kunde seine Daten bei sich vor Ort speichert, kann Swisscom Empfehlungen abgeben, wie diese Räume zu sichern sind. Es liegt in der Verantwortung des Kunden die nötigen Schutzmassnahmen zu treffen.

2.3 Zugangskontrolle

[1] Der Zugriff auf die Systeme von Swisscom erfolgt immer mit personalisierten Identifikationen der beauftragten Personen von Swisscom.

[2] Der Zugang zu den Systemen ist immer mindestens mit einem Passwort oder einem äquivalenten Authentisierungsmerkmal und der dazu gehörenden digitalen Identifikation geschützt. Die Zugangsdaten werden so gespeichert, dass keine

direkte Ableitung des gültigen Authentisierungsmerkmals möglich ist, falls diese Daten zugreifbar würden.

3 Die Passwörter müssen komplexe Anforderungen erfüllen und bestehen mindestens aus drei Klassen der folgenden Elemente: grossgeschriebene Buchstaben, kleingeschriebene Buchstaben, Zahlen, Sonderzeichen. Passwörter persönlicher Accounts werden nie an Dritte zugänglich gemacht.

4 Bei fehlerhafter Anmeldung kann die Identifikation zuerst temporär und nach weiteren Fehlversuchen permanent gesperrt werden.

5 Über Internet zugängliche Portale verlangen in Abhängigkeit derer Klassifizierung von Benutzern eine starke Authentisierung beim Zugriff auf die relevanten Daten. Die starke Authentisierung basiert dabei auf Mobile ID, Verwendung eines elektronischen Tokens zur Generierung von Einmal-Passwörtern oder anderen sicheren Mitteln als zweiter Faktor.

2.4 Zugriffskontrolle

1 Die Berechtigungen auf den Systemen werden in Rollen strukturiert. Eine Identität erhält eine oder mehrere Rollen zugewiesen, die für die Ausführung der Organisationsrolle der Person nötig sind. Die Rollen sind so strukturiert, dass nur auf die Daten zugegriffen werden kann, die für die Erfüllung der Aufgabe nötig sind. Die Beschreibung der Rollen und ihrer Berechtigungen sind in Rollenkonzepten dokumentiert.

2 Falls ein Mitarbeiter zusätzliche Rechte benötigt, kann er eine zusätzliche Rolle bestellen. Die Freigabe für diese zusätzliche Rolle erfolgt durch den Vorgesetzten und den Rollenbesitzer. Der Rollenbesitzer kann entscheiden ob diese Freigabe effektiv nötig ist, oder eine automatische Freigabe erfolgen kann. Eine sehr limitierte Anzahl Rollen werden automatisch dem Mitarbeiter zugeordnet, dabei handelt es sich Rollen aus der Organisationsstruktur, wie z.B. die Zugehörigkeit in eine Organisationseinheit.

3 Der Datenverkehr zwischen dem Netzwerk des Kunden und Swisscom erfolgt nach Möglichkeit verschlüsselt oder wird durch alternative Massnahmen geschützt. Alternative Massnahmen können z.B. die Verwendung von dedizierten logischen Leitungen oder die Verwendung von direkten Glasfaserverbindungen sein. Die Verschlüsselung der Verbindung basiert auf aktuellen Protokollen und Schutzmechanismen.

4 Zugriffe auf die Systeme werden protokolliert und können mit verschiedenen Verfahren analysiert werden.

2.5 Transportkontrolle

1 Der Zugriff über das Internet auf relevante Daten erfolgt immer über eine verschlüsselte Verbindung. Dabei verwendet Swisscom aktuelle Protokolle und Schutzmechanismen. Diese verschlüsselte Verbindung basiert auf Technologien auf Netzwerk-, Session- oder Anwendungsschicht.

2 Der direkte Zugriff des Kunden auf seine personenbezogenen Daten wird nach Vereinbarung mit dem Kunden über den Transportweg geschützt. Swisscom bietet hier entsprechende Services an, die virtuelle Netzwerkverbindungen zum Kunden ermöglichen. Zusätzlich können für diese Verbindungen auch noch weitere Verschlüsselungstechniken eingesetzt werden.

2.6 Speicherkontrolle

1 Die permanenten Speicher in den Rechenzentren werden mit physischen Schutzmassnahmen gegen Verlust geschützt. Dazu gehören redundante Stromversorgungen und die notwendigen Systeme um einen autarken Betrieb für einen definierten Zeitraum zu ermöglichen.

2 Zum Schutz vor Rauch- oder Brandschäden verfügen die hochsicheren Räume über Rauch- und Brandmeldeanlagen. Im Ereignisfall wird entweder für eine Erstreaktion das anwesende Sicherheitspersonal respektive Gebäudepersonal eingesetzt oder eine Löschanlage aktiviert, um den potentiellen Schaden möglichst gering zu halten. Falls kein Personal vor Ort vorhanden ist wird der Alarm an die lokale Feuerwehr geleitet.

3 Datenträger werden bei Defekt von Swisscom physisch unbrauchbar gemacht, um einen möglichen Zugriff vollständig auszuschliessen.

4 Funktionierende Datenträger werden mit branchenüblichen Löschverfahren so gelöscht, dass eine Rekonstruktion der beinhalteten Daten beinahe unmöglich ist. Ist ein solches Verfahren nicht möglich, werden die Datenträger physisch unbrauchbar gemacht, respektive zerstört.

5 Eine Rückgabe von Datenträger an den Kunden ist unter definierten Umständen möglich. Dies bedingt, dass das Speichersystem, respektive der Datenträger nur für diesen einen Kunden im Einsatz gestanden ist.

2.7 Eingabekontrolle

1 Swisscom stellt für den Fall, in dem Swisscom für die Eingabe und Verarbeitung von personenbezogenen Daten zuständig ist, mit den notwendigen Massnahmen sicher, dass diese Daten korrekt erfasst und verarbeitet werden.

2 Swisscom erfasst für die Service-Erbringung weitere personenbezogene Daten des Kunden in Systemen von Swisscom. Diese Systeme dienen z.B. zur Erfassung von Fehlermeldungen (Incidents), Erfassung von Änderungswünschen oder zur Rechnungsstellung. Swisscom stellt durch geeignete Qualitätsmassnahmen sicher, dass relevante Daten, die hierbei erfasst werden, geprüft und korrigiert werden.

2.8 Auftragskontrolle

1 Swisscom wählt mögliche Unterlieferanten mit Zugriff auf die Daten sorgfältig aus und überbindet die relevanten Verantwortlichkeiten zum Datenschutz den Lieferanten.

2 Swisscom hat für die Gewährleistung der Datenschutz-Anforderungen eine verantwortliche Organisation benannt. Diese ist für Anfragen unter datenschutz.sbc@swisscom.com erreichbar. Erste Ansprechstelle für Fragen zum Datenschutz bei Swisscom ist der zuständige Account Manager von Swisscom.

3 Neue Mitarbeiter von Swisscom werden vor Beginn ihrer Anstellung einer Sicherheitsprüfung unterzogen. Diese besteht aus verschiedenen Stufen und ist je nach Zugriffsmöglichkeit auf relevante Daten unterschiedlich ausgestaltet. Die Prüfung umfasst mindestens die Verifikation des vollständigen Lebenslaufs, der letzten Zeugnisse und das Einholen einer persönlichen Referenzauskunft.
In den weiteren Stufen kommen hier noch das Unterzeichnen einer Vertraulichkeitserklärung oder eine Überprüfung gemäss Personensicherheitsüberprüfung des Bundes dazu.

4 Neue Mitarbeiter werden bei ihrem Arbeitsbeginn mit den relevanten Regeln zur eigenen Sicherheit und zur Datensicherheit vertraut gemacht.

5 Bestehende Mitarbeiter von Swisscom werden regelmässig zum sorgfältigen Umgang mit Daten geschult. Dazu dienen Meldungen im Intranet, Blogbeiträge, elektronische Awareness-Schulungen auf der Lernplattform von Swisscom wie auch vor-Ort-Schulungen.

6 Wenn der Swisscom Mitarbeiter die Firma verlässt, wird die Hauptidentität auf den Systemen von Swisscom automatisch gesperrt. Der Zutritt zu den Gebäuden wird ebenfalls am Ende des letzten Arbeitstags gesperrt. Es ist die Aufgabe des Vorgesetzten, sämtliche weiteren Zugriffe zu löschen und am letzten Arbeitstag des Mitarbeiters den Badge und die Arbeitsgeräte von Swisscom einzuziehen.

2.9 Verfügbarkeitskontrolle

1 Swisscom speichert die Daten gemäss vertraglicher Vereinbarung in Rechenzentren mit dem notwendigen Schutzniveau.

Dabei kann es sich um Rechenzentren von Swisscom oder Dritten handeln).

2 Um die Verfügbarkeit der Daten zu gewährleisten, werden die Speichersysteme von Swisscom so konfiguriert, dass auch mehr als eine Komponente ausfallen kann und die Daten trotzdem noch verfügbar sind. Dies wird durch redundante, verteilte Datenträger wie auch redundante Netzwerke und Stromversorgungen erreicht.

3 Swisscom sichert die Daten gemäss der Servicebeschreibung. Dabei kann die Sicherung auf Speichersystemen in einem weiteren Rechenzentrum mit einer genügenden geografischen Distanz zwischen den beiden Standorten erfolgen. Die unterschiedlichen geografischen Räume dienen dazu, mögliche Schäden durch Naturereignisse wie Blitz, Regen, Überschwemmung, Murgänge auf möglichst einen Standort zu minimieren.

4 Abhängig von den bezogenen Leistungen kann der Kunde unterschiedliche Niveaus von Datensicherungen zusätzlich bestellen. Dies ist in der Servicebeschreibung ersichtlich oder kann beim Account Manager von Swisscom nachgefragt werden.

5 Swisscom hat die nötigen Prozesse implementiert, um Meldungen über Softwareschwachstellen und Patches zu identifizieren, zu bewerten und daraus notwendigen weiteren Schritte abzuleiten.

2.10 Trennungsgebot

1 Swisscom stellt sicher, dass die Daten der Kunden nicht gegenseitig einsehbar sind. Dazu werden aktuelle Sicherheitsverfahren eingesetzt, die auf logischer oder physischer Ebene die Trennung der Kundendaten sicherstellen.

2 Physische Verfahren sind dann angebracht, wenn der Service und die dazu verwendeten Systeme es nicht erlauben, eine adäquate logische Trennung zu ermöglichen. Swisscom versucht aus Kostengründen möglichst immer logische Verfahren einzusetzen.

3 Je nach Service Angebot kann der Kunde von sich aus den Wunsch äussern, dass seine Daten physisch von den Daten anderer Kunden getrennt werden. Diese Option ist nicht in allen Angeboten verfügbar.

4 Logische Verfahren sind von Swisscom darauf geprüft worden, dass diese Verfahren nicht ausgehebelt werden können. Falls Swisscom feststellen würde, dass die Verfahren dies nicht mehr gewährleisten, wird Swisscom die nötigen Gegenmassnahmen treffen um einen äquivalenten Schutz wiederherzustellen.

2.11 Überprüfung, Bewertung und Evaluierung

1 Swisscom führt regelmässige System-Audits durch. Im technischen Bereich ist das z.B. eine regelmässige Überprüfung des IP-Perimeters oder Securityaudits von Plattformen.

2 Basierend auf einer Risiko-Analyse werden neue Leistungen und Dienste einer technischen Prüfung unterzogen. Festgestellte Mängel werden von den verantwortlichen Stellen behoben. Je nach Schwere der Mängel wird eine ergänzende Prüfung durchgeführt, um die Wirksamkeit der Behebung nachzuweisen.

3 Swisscom führt über das ganze Unternehmen ein Risikomanagement-System, um Risiken festzustellen, zu quantifizieren und zusammen mit den verantwortlichen Organisationen Massnahmen zur Reduktion der Risiken einzuleiten.

4 Swisscom nimmt am einen Bug Bounty Programm teil. Dieses ermöglicht es jedermann erkannte Sicherheitslücken in den Services von Swisscom zentralisiert zu melden. Die Meldungen werden evaluiert und die nötigen Gegenmassnahmen getroffen, z.B. ein Patch für eine Software erstellt oder der Code einer Webseite verbessert.