

## Anhang 7 Auftragsdatenverarbeitung

<b>Version</b>	1.0
<b>Ausgabedatum</b>	28.04.2023
<b>Ersetzt Version</b>	-
<b>Änderungen</b>	Neues Dokument
<b>Gültig ab</b>	01.07.2023

### 1. Einleitung

Der vorliegende Anhang konkretisiert die Verpflichtungen der Parteien in Bezug auf die Vorgaben aus dem schweizerischen Datenschutzgesetz (DSG) ([6] Anhang 4) und der Europäischen Datenschutzgrundverordnung (EU-DSGVO 2016R0679) ([9] Anhang 4). Er ergänzt die Teldas Verträge «Benutzung des TSP INET-Servers beim Wechsel der FDA für Nummern (Nummernportierung)» und «Benutzung des TSP INet-Servers für INA-Dienste».

Teldas (Auftragsbearbeiter) bearbeitet im Auftrag des Benutzers (Verantwortliche) personenbezogene Daten („relevante Daten“) gemäss den Bestimmungen dieses Anhanges.

### 2. Gegenstand und Dauer der Vereinbarung

Der Gegenstand des Auftrages sowie Art und Zweck der Bearbeitung ergeben sich aus dem Benutzervertrag.

Die vorliegende Vereinbarung tritt mit gegenseitiger Unterzeichnung des Benutzervertrages in Kraft. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages «Benutzung des TSP INET-Servers beim Wechsel der FDA bzw. des Benutzers für Nummern (Nummernportierung)» und/oder «Benutzung des TSP INet-Servers für INA-Dienste».

Die Pflichten aus dieser Vereinbarung gelten zusätzlich zu die im Vertrag «Benutzung des TSP INET-Servers beim Wechsel der FDA für Nummern (Nummernportierung)» und/oder «Benutzung des TSP INet-Servers für INA-Dienste» festgelegten Pflichten und schränken letztere nicht ein. In Bezug auf die in einer Beilage zu dieser Vereinbarung generisch festgelegten Technisch-organisatorischen Massnahmen (TOM) gehen im Widerspruchsfall die Regelungen dieser Vereinbarung vor.

### 3. Pflichten der Teldas

- (1) Teldas verarbeitet personenbezogene Daten ausschliesslich gemäss den Bestimmungen dieser Vereinbarung oder allfälligen weiteren dokumentierter Weisungen des Benutzers, es sei denn, Teldas ist gesetzlich zu einer weiteren Verarbeitung verpflichtet. Teldas teilt solche Pflichten dem Benutzer vor der Verarbeitung mit, es sei denn, das betreffende Recht verbietet eine solche Mitteilung wegen eines wichtigen öffentlichen Interesses.
- (2) Teldas informiert den Benutzer umgehend, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstösst. Teldas ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Benutzer bei der Teldas nach Überprüfung bestätigt oder geändert wird.
- (3) Die Weisungen werden anfänglich in dieser Vereinbarung festgelegt und können vom Benutzer in der Folge in schriftlicher Form oder in einem elektronischen Format (Textform) an der Teldas durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung) soweit diese im Rahmen der vertraglich vereinbarten Leistungen durch Teldas umsetzbar und objektiv zumutbar sind. Führen solche Weisungen zu Mehrkosten von Teldas oder einem geänderten Leistungsumfang, so ist das vertragliche Vertragsänderungsverfahren anwendbar.

- (4) Teldas verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Zustimmung des Benutzers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
- (5) Teldas verpflichtet sich im Rahmen der Datenverarbeitung die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften zu beachten. Teldas bestätigt, dass den von ihr zur Datenverarbeitung eingesetzten Personen die relevanten Bestimmungen des Datenschutzes und dieser Vereinbarung vertraut sind. Entsprechende Schulungs- und Sensibilisierungsmassnahmen haben in regelmässigen Abständen zu erfolgen.
- (6) Teldas erklärt rechtsverbindlich, dass sie alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden bei der Teldas (oder Unterauftragsverarbeiter) aufrecht.
- (7) Teldas unterstützt den Benutzer im erforderlichen Ausmass bei der Gewährung der Rechte der betroffenen Personen nach Kapitel 4 DSG bzw. Kapitel 3 EU-DSGVO, damit der Benutzer innerhalb der gesetzlichen Fristen seine Aufgaben jederzeit erfüllen kann und überlässt dem Benutzer alle dafür notwendigen Informationen. Falls eine betroffene Person eine Anfrage direkt an der Teldas sendet, leitet diese die Anfrage umgehend an den Benutzer weiter. Auskünfte an Dritte oder Betroffene darf Teldas nur nach vorheriger Zustimmung durch den Benutzer erteilen.
- (8) Teldas unterstützt den Benutzer bei der Einhaltung der in den Art. 22-24 DSG bzw. Art. 32 bis 36 EU-DSGVO genannten Pflichten (Datensicherheitsmassnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation). Mitunter unterrichtet Teldas den Benutzer unverzüglich, wenn ihm Verletzungen des Schutzes der relevanten Daten bei ihm oder einem seiner Unter-Auftragsbearbeiter bekannt werden (Data Breach).
- (9) Wird der Benutzer durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen, verpflichtet sich Teldas, den Benutzer im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
- (10) Teldas hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Benutzer dies verlangt und keine berechtigten Interessen der Teldas oder gesetzliche Vorgaben dem entgegenstehen.
- (11) Teldas hat keinen Datenschutzverantwortlichen nach Art. 37 EU-DSGVO bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt. Der Ansprechpartner für Datenschutzfragen bei der Teldas ist im Anhang 1 aufgeführt.

#### **4. Unterauftragsverarbeiter**

- (1) Teldas ist zum Beizug von Unterauftragslieferanten berechtigt, hat jedoch den Benutzer vorgängig darüber zu informieren, wenn sie nach Inkrafttreten dieser Vereinbarung neue Unterauftragsverarbeiter beizieht bzw. bestehende austauscht. Die Liste der Unterauftragsverarbeiter ist im Anhang 2 Punkt 6 veröffentlicht.
- (2) Der Benutzer kann gegen den Bezug eines neuen Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichem Grund schriftlich innerhalb einer Frist von 30 Tagen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche

Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Benutzer ein Kündigungsrecht in Bezug auf die hiervon betroffene Leistung eingeräumt.

- (3) Teldas wird mit ihren Unterauftragsverarbeitern im erforderlichen Umfang Vereinbarungen treffen, um die Verpflichtungen gemäss vorliegende Vereinbarung sicherzustellen.
- (4) Dem Benutzer ist auf Anfrage Einsicht in die relevanten Datenschutzbestimmungen zwischen der Teldas und dem Unterauftragsverarbeiter zu gewähren.
- (5) Der Benutzer ist bei begründetem Verdacht bezüglich der auf Verletzung der niedergelegten Pflichten berechtigt, in dem hier festgelegten Umfang Kontrollen auch bei Unterauftragsverarbeitern durchzuführen oder durch Dritte durchführen zu lassen. Auf jeden Fall ist im Rahmen solcher Kontrollen der Grundsatz der Verhältnismässigkeit einzuhalten sowie die schutzwürdigen Interessen von Teldas sowie deren Unterauftragsverarbeitern (namentlich auf Geheimhaltung) angemessen zu berücksichtigen.
- (6) Teldas ist für die Rechtmässigkeit der Datenverarbeitung an sich, inklusive der Zulässigkeit der Unterauftragsverarbeitung, verantwortlich.

## **5. Technische und organisatorische Massnahmen (TOM)**

- (1) Teldas ergreift alle erforderlichen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 8 DSG bzw. Art. 32 EU-DSGVO. Die Massnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.
- (2) Die erforderlichen technischen und organisatorischen Massnahmen sind in der Beilage 1 zu dieser Vereinbarung dokumentiert.
- (3) Wesentliche Änderungen sind ebenfalls umgehend zu dokumentieren. Teldas darf die vereinbarten TOM jederzeit anpassen, solange das vereinbarte Schutzniveau nicht unterschritten wird (vgl. Ziffer 9 Änderungen der Vereinbarung).
- (4) Soweit die getroffenen Sicherheitsmassnahmen den Anforderungen des Benutzers nicht oder nicht mehr genügen, benachrichtigt letzterer die Teldas schriftlich.

## **6. Verpflichtungen der Teldas nach Beendigung des Auftrags**

- (1) Teldas ist nach Beendigung der Auftragsverarbeitung verpflichtet, alle Verarbeitungsergebnisse und übermittelten personenbezogenen Daten und deren Kopien, im Benutzer Auftrag zu vernichten, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht (wie per Art. 28 Abs. 3 Satz 2 Bst. G EU-DSGVO). Die Kundendaten sind in sogenannten Work-Order Dateien enthalten. Die Datenspeicherungslänge ist im Dokument „Archiving Rules“ festgelegt (Siehe <https://extranet.teldas.ch/documents>).
- (2) Wenn Teldas die Daten in einem speziellen technischen Format verarbeitet, ist sie verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Benutzers in dem Format, in dem sie die Daten vom Benutzer erhalten hat oder in einem anderen, gängigen Format zurückzugeben. Die Kundendaten sind in sogenannten Work-Order Dateien enthalten. Die Daten können via eine Web-basierte manuelle Schnittstelle oder via WS in einem gängigen Format runtergeladen werden (Siehe Spezifikationen unter <https://extranet.teldas.ch/documents>).

## 7. Nachweismöglichkeiten, Berichte und Audits

Der Benutzer ist berechtigt:

- (1) die Einhaltung der von der Teldas getroffenen technischen und organisatorischen Massnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen in angemessenem Umfang selbst oder durch Dritte vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist von der Teldas soweit erforderlich Zutritt und Einblick zu ermöglichen. Teldas erteilt die erforderlichen Auskünfte, um die Einhaltung der vereinbarten Pflichten zu dokumentieren. Auf jeden Fall ist im Rahmen solcher Kontrollen der Grundsatz der Verhältnismässigkeit einzuhalten sowie die schutzwürdigen Interessen von Teldas (namentlich auf Geheimhaltung) angemessen zu berücksichtigen.
- (2) Kontrollen bei der Teldas erfolgen ohne vermeidbare Störungen ihres Geschäftsbetriebs und ausser bei dringlichen Gründen nach angemessener Vorankündigung und während der Geschäftszeiten der Teldas.
- (3) Vorbehältlich einer abweichenden Regelung trägt der Benutzer sämtliche Kosten solcher Audits (inklusive nachgewiesene interne Kosten von Teldas, die bei der Mitwirkung am Audit entstehen).
- (4) Werden nach Vorlage von Nachweisen oder Berichten oder im Rahmen eines Audits Verletzungen dieser Vereinbarung oder Mängel bei der Umsetzung der Pflichten festgestellt, so muss Teldas unverzüglich und kostenlos geeignete Korrekturmassnahmen implementieren.

## 8. Pflichten des Benutzers

Der Benutzer ist verpflichtet:

- (1) sicher zu stellen, dass die Rechtmässigkeit der Verarbeitung gemäss Art. 6 Abs. 1 DSG bzw. Art. 6 Abs. 1 EU-DSGVO gegeben ist;
- (2) zu gewährleisten, dass die Rechte der betroffenen Personen nach Kapitel 4 DSG bzw. Kapitel 3 EU-DSGVO gewahrt werden.
- (3) der Teldas Aufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format zu übermitteln. Mündliche Weisungen sind schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen;
- (4) Teldas unverzüglich über Fehler oder Unregelmässigkeiten bei der Prüfung der Auftragsergebnisse zu informieren;
- (5) alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der Teldas vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrages bestehen.
- (6) den Ansprechpartner zu nennen für im Rahmen des Vertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten. Siehe Anhang 1.

## 9. Änderung der Vereinbarung

Der Benutzer kann von TELDAS Änderungen (inklusive Ergänzungen) dieser Vereinbarung fordern, falls und soweit dies zur Einhaltung von durch die Benutzer einzuhaltendem zwingendem Datenschutzrecht erforderlich ist.

TELDAS informiert die Benutzer frühzeitig mittels Email über erforderliche Anpassungen oder Ergänzungen der Beilagen 1 und 2. Die Änderungen gelten als genehmigt, wenn der Benutzer sie nicht innerhalb von 30 Tage ab Erhalt aus wichtigen Gründen widerspricht.

## Beilage 1: Technisch-organisatorische Massnahmen (TOM)

Die folgenden Kapitel beschreiben die von Teldas getroffenen Massnahmen in Bezug auf den Schutz von personenbezogenen Daten gemäss Art. 8 DSG bzw. 32 EU-DSGVO). Die Beurteilung, ob die nachfolgend beschriebenen technischen und organisatorischen Massnahmen zum Schutz der Teldas zur Bearbeitung anvertrauten Daten angemessen sind, obliegt ausschliesslich dem Benutzer.

Jede Partei bearbeitet im Rahmen der Vertragsbeziehung Personendaten über Mitarbeitende und andere Hilfspersonen der anderen Partei. Für die Zwecke der Vertragsabwicklung und Pflege der Vertragsbeziehung bearbeiten die Parteien diese Personendaten in gemeinsamer Verantwortlichkeit auf ihren jeweils eigenen Systemen und unter Anwendung von angemessenen technischen und organisatorischen Massnahmen zum Schutz der Daten. Diese Art von Datenbearbeitung unterliegen nicht den Regelungen der Auftragsdatenbearbeitung. Kontakte von Mitarbeitenden oder anderen Hilfspersonen der Benutzer werden für andere Benutzer der Teldas zugänglich gemacht für notwendige operationelle, administrative und Verrechnungszwecke zwischen Anbietern.

### 1. Vertraulichkeit

- (1) **Zutrittskontrolle:** Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.

Die INet-Datenbank ist in einem gesicherten Rechenzentrum des Teldas Unterauftragsverarbeiters gelagert, Siehe Data Center DSC Wankdorf der Swisscom: <https://www.swisscom.ch/fr/about/entreprise/durabilite/objectifs-cr-et-resultats/centre-de-calcul-wankdorf.html> und Tier4 Zertifizierung durch externen Organismus: <https://uptimeinstitute.com/TierCertification/allCertifications.php?page=1&ipp=All&clientId=251&countryName=&tierLevel=>.

Um in gesicherte Zonen Zutritt zu erhalten, wird ein Badge oder Schlüssel benötigt. Die Ausgabe der Schlüssel an die berechtigten Personen wird protokolliert, und Besucher müssen sich registrieren und werden in den gesicherten Zonen von den verantwortlichen Mitarbeitenden begleitet.

- (2) **Zugangskontrolle:** Keine unbefugte Systembenutzung.

Der Zugriff auf die Systeme von Teldas erfolgt immer mit personalisierten Identifikationen der beauftragten Personen von Teldas.

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.

Die Passwörter müssen komplexe Anforderungen erfüllen, 8 Charakter lang sein und bestehen mindestens aus drei Klassen der folgenden Elemente: grossgeschriebene Buchstaben, kleingeschriebene Buchstaben, Zahlen, Sonderzeichen.

- (3) **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.

Der Zugriff auf dem INet-Server der Teldas basiert auf Berechtigungen der Benutzer mit Zuordnung verschiedener Rollen. Die Kundendateien sind nur für die vom Portierungsauftrag betroffenen Anbietern (Donor und Recipient) und berechnigte Personen (Teldas Helpdesk und Support Teams) verfügbar. Logs der Zugriffe werden für eine definierten Zeitspanne gespeichert.

Der Zugriff mit erhöhten Rechten zur Administration des INet-Systems der Teldas ist mit starker Zwei-Faktor-Authentisierung abgebildet. Alle Anmeldungen, Abmeldungen und fehlerhafte Anmeldungen werden zentral protokolliert und für eine definierte Zeitspanne gespeichert.

Zugriffe auf die Systeme werden zentral protokolliert und bei Bedarf analysiert.

- (4) **Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Teldas stellt sicher, dass die Daten der Benutzer nicht gegenseitig einsehbar sind. Dazu werden aktuelle Sicherheitsverfahren eingesetzt, die auf logischer Ebene die Trennung der Benutzerdaten sicherstellen.

Work-Order Dateien werden von Portierungen-Dateien getrennt. Nur Donor und Recipient können Details Ihrer Work-Order Datei einsehen.

## 2. Integrität

- (1) **Transportkontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.

Persönliche Daten werden vom „Recipient“ geliefert mit Zwei-Faktor-Authentifizierung über das WebSite oder mittels HTTPS gesicherte und verschlüsselte Verbindung (SSL) via einem Web Service Zugriff.

- (2) **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Der Benutzer ist für die korrekte Handhabung und Änderung der Daten verantwortlich. Generierung und Änderungen von WO-Dateien werden protokolliert (Benutzer-Id ist in der WO-Datei ersichtlich).

## 3. Verfügbarkeit und Belastbarkeit

- (1) **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.

Daten werden auf Harddisk-Systeme in einem weiteren Rechenzentrum gesichert mit einer genügenden geographischen Distanz zwischen den beiden Standorten.

Unterbrechungsfreie Stromversorgung: Das INet-System ist in einem Pier 4 Rechenzentrum der Swisscom untergebracht. 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.

Backup-Strategie (online/offline; on-site/off-site): regelmässige Back-ups werden durchgeführt um den Datenverlust zu minimieren. Das INet-System wird alle 4 Stunden einem Back-up unterzogen.

Virenschutz, Firewall sind vorhanden.

Der Standard Patch-Management Prozess stellt sicher, dass Ankündigungen von Patches bewertet und nach einer Prüfung auf den relevanten Systemen installiert werden.

- (2) **Rasche Wiederherstellbarkeit:** Datenbank kann temporär auf Cloud-Umgebung innerhalb von 24 Stunden wiederhergestellt werden. Ein Notfallplan ist vorhanden, um das System wieder innerhalb von 24 Stunden betriebsbereit zu machen.

#### 4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

- (1) **Datenschutz-Management:** periodische Sitzungen zwischen Teldas und Teldas Unterauftragsverarbeitern finden statt. Der Teldas Hauptunterauftragsverarbeiter (Swisscom) untersteht einem jährlichen Bericht ISAE3402 basierend auf einem Audit von PWC.
- (2) **Incident-Response-Management:** Die Benutzer können Fehlern bei der Teldas Helpdesk melden und Tickets werden dann eröffnet und verfolgt.
- (3) **Datenschutzfreundliche Voreinstellungen** bei jedem neuen Projekt werden die Sicherheits- und Datenschutzaspekte vorrangig berücksichtigt.
- (4) **Auftragskontrolle:** Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Benutzers.

Teldas wählt mögliche Unterlieferanten mit Zugriff auf die Daten sorgfältig aus und überbindet die relevanten Verantwortlichkeiten zum Datenschutz den Lieferanten. Die neuen Unterlieferanten von Teldas werden dem Benutzer für jeden einzelnen bezogenen Service namentlich genannt.

- (5) **Sicherheitsaudits** werden periodisch in Auftrag gegeben. Sicherheitsrisiken werden bewertet, quantifiziert und priorisiert.

## **Beilage 2: Beschreibung der Datenbearbeitung**

### **1. Ort der Durchführung der Auftragsverarbeitung**

Alle Datenverarbeitungstätigkeiten werden ausschliesslich innerhalb der Schweiz durchgeführt.

Das angemessene Datenschutzniveau der Schweiz ergibt sich aus einem Angemessenheitsbeschluss vom 26. Juli 2000 der Europäischen Kommission nach Art. 45 EU-DSGVO.

### **2. Kategorien von Daten und betroffener Personen**

Der Benutzer macht Teldas im Rahmen der Nummernportierungsdienstleistung und INA-Dienstleistung personenbezogene Daten zur Verarbeitung zugänglich. Es betrifft Endkundendaten der Inhaber von offiziellen Telefonnummern und die den Anbieter wechseln möchten.

Die vom Benutzer übermittelten personenbezogenen Daten (Art. 5a DSG bzw. Art. 4 Nr 1 EU-DSGVO) gehören zu folgenden Datenkategorien:

- Persönliche Informationen wie Nachname, Vorname
- Private oder Geschäftliche Kontaktdaten, wie Telefonnummer, Adresse.
- INA-Referenz-Code vom Bakom an den INA-Nummerninhaber vergeben

Teldas und Ihre Unter-Auftragsbearbeiter bearbeiten keine relevanten Daten, welche einer spezialgesetzlichen Geheimhaltungspflicht unterliegen.

### **3. Art der Verarbeitung**

Die Bearbeitung der Endkundendaten betrifft Portierungsdaten (Name, Vorname, Adresse, Telefonnummer) des Kunden, die in so-genannte WO-Dateien gespeichert werden und Teil des Portierungsprozesses sind. Im Fall von Problemen bei der Portierung, kann man die Historie verfolgen. Die übermittelten personenbezogenen Daten werden von der Teldas nicht geändert. Daten werden vom neuen Anbieter („Recipient“) eingegeben und sind für den aktuellen Anbieter („Donor“) sichtbar, werden von ihm oder vom System aber nicht geändert.

Die Datenspeicherungslänge und Löschung der Kundendaten ist im Dokument [13] Anhang 4 festgelegt.

### **4. Verarbeitungszwecke**

Teldas verarbeitet die relevanten Daten ausschliesslich gemäss den Bestimmungen aus dem Vertrag «Benutzung des TSP INET-Servers beim Wechsel der FDA für Nummern (Nummernportierung)» und „Benutzung des TSP INet-Servers für INA-Dienste“. Vorbehalten bleibt die Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch Teldas.

Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken verarbeitet:

- Nummernportierung (Siehe [15] Anhang 4). Person bezogene Kundendaten werden nicht öffentlich publiziert und sind immer nur für den neuen („Recipient“) und aktuellen („Donor“) Anbieter sichtbar. Sie werden benutzt, um den Vertrag beim aktuellen Anbieter zu kündigen.
- INA-Prozesse (Siehe [18] Anhang 4).
- So-genannte WO-Dateien werden für die Verrechnung zwischen Anbieterinnen für SLA-Streitigkeiten benötigt, sowie für die Verrechnung der Transaktionsbasierende Gebühren durch die Teldas an den Benutzer.



## 5. Offenlegung relevanter Daten an Unter-Auftragsbearbeiter (z.B. Gruppengesellschaften, Lieferanten)

Hiernach die Liste der Teldas Unter-Auftragsbearbeiter mit einer Beschreibung der Art von persönlichen Daten welche bearbeitet werden:

Firma	Adresse	Land	Umfang der Bearbeitung
MNC Mobile News Channel SA	Avenue de la Gare 10, 1003 Lausanne	CH	Outsourcing-Partner für SMS-Versand und -Empfang
Swisscom (Schweiz) AG	Alte Tiefenaustrasse 6, 3050 Bern	CH	Outsourcing-Partner für Applikationsbetrieb
Open Web Technology SA	Avenue de Rhodanie 40C Building C, 4th floor, 1007 Lausanne	CH	Outsourcing-Partner für Applikationsmanagement

## 6. Meldung von Datenschutzverstösse /Sicherheits Incident

Teldas meldet Datenschutzverstösse durch eine ITBd Meldung, die Benutzer unter dem Teldas Extranet abonnieren können (<https://extranet.teldas.ch/account>).