Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG)

(veröffentlicht Juni 2021)

1. Zweck der Anleitung

Die vorliegende Anleitung soll Datenbearbeitern die Prüfung der Zulässigkeit von Datenübermittlungen von personenbezogenen Daten ins Ausland erleichtern.

Anhand eines Schemas erläutert diese Anleitung den Anwendungsfall des Datentransfers ins Ausland nach Art. 6 Abs. 2 lit. a DSG, wenn dort eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, und dieser Mangel durch hinreichende Garantien kompensiert werden muss (vgl. auch Art. 6 Abs. 2 und 3 der Verordnung zum Bundesgesetz über den Datenschutz VDSG, SR. 235.11). Auf die Voraussetzungen nach lit. b – g wird in dieser Anleitung nicht eingegangen.

SR 235.1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)

Art. 6 Grenzüberschreitende Bekanntgabe

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

[2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten.

SR 235.11 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG)

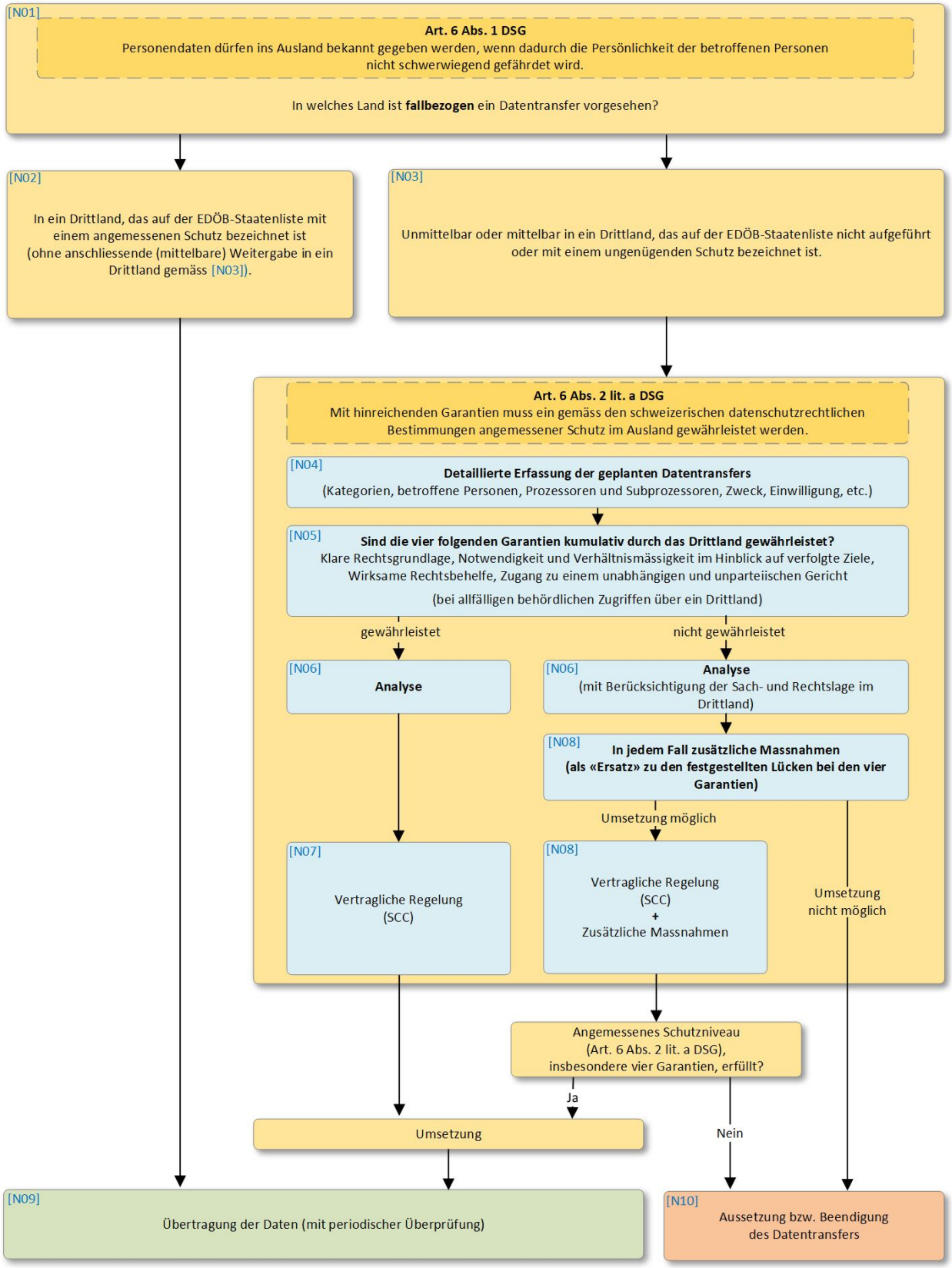
Art. 6 Informationspflicht

[2] Wurde der Beauftragte über die Garantien und die Datenschutzregeln informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:

a. unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder
b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden, soweit die Datenschutzregeln weiterhin einen angemessenen Schutz gewährleisten.

[3] Die Informationspflicht gilt ebenfalls als erfüllt, wenn Daten gestützt auf Musterverträge oder Standardvertragsklauseln übermittelt werden, die vom Beauftragten erstellt oder anerkannt wurden, und der Beauftragte vom Inhaber der Datensammlung in allgemeiner Form über die Verwendung dieser Musterverträge oder Standardvertragsklauseln informiert wurde. Der Beauftragte veröffentlicht eine Liste der von ihm erstellten oder anerkannten Musterverträge und Standardvertragsklauseln.

2. Ablaufschema



3. Erläuterungen

[N01] Überprüfung des Datenschutzniveaus im Drittland

Der verantwortliche Datenexporteur muss sicherstellen, dass bei der Bearbeitung der Daten in den Zielländern ein angemessenes Datenschutzniveau gewährleistet ist (Art. 6 DSG). Wenn die Daten in ein EU/EWR Land transferiert werden, kann von einem angemessenen Datenschutzniveau ausgegangen werden, wenn ein Weiterexport in ein Drittland ausgeschlossen ist.

Es ist zu beachten, dass ein Auftragsdatenbearbeiter bzw. –prozessor in einem Land mit angemessenem Datenschutzniveau unter Umständen einem Gesetz oder anderen zwingenden Vorgaben eines Drittlandes unterstehen kann, das diesen zur Bekanntgabe der Daten an die Behörden eines Drittlandes verpflichtet und diese Bekanntgaben z.B. intransparent oder nicht justiziabel sind (vgl. dazu im Einzelnen die Garantien in N05). In diesem Fall ist nach N03 zu verfahren (Bsp.: Server in der Schweiz, EU oder dem EWR eines Unternehmens, welches direkt oder indirekt einer staatlichen Rechtsordnung eines Staates ohne angemessenem Datenschutzniveau untersteht).

[N02] Angemessenheit (Art. 6 Abs. 1 DSG)

Exportstaat figuriert auf der EDÖB Staatenliste

Wenn der Inhaber von Datensammlungen Daten in einen Staat übermittelt, der auf der Staatenliste des EDÖB als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird, gilt er als gutgläubig gemäss Art. 3 Abs. 1 ZGB. Allerdings handelt es sich um eine widerlegbare Vermutung. Der Inhaber der Datensammlung kann sich dann nicht auf seinen guten Glauben berufen, wenn er z.B. Kenntnis hat, dass in seinem spezifischen Fall das angemessene Datenschutzniveau in einem bestimmten Land dennoch nicht gewährleistet ist (Art. 3 Abs. 2 ZGB).

Der Datenexporteuer bleibt in jedem Fall für den Datenexport verantwortlich und muss sich periodisch darüber informieren, ob die Angemessenheit nach wie vor gilt und dass nicht andere Gründe (z.B. aufgrund von Hinweisen aus der Praxis oder den Medien) gegen eine sichere Bearbeitung der Personendaten im entsprechenden Zielland sprechen.

Exportstaat figuriert nicht auf der EDÖB Staatenliste

Figuriert ein Staat nicht auf der Staatenliste des EDÖB, bedeutet dies nicht automatisch, dass er keinen angemessenen Schutz gewährleistet. Der EDÖB hat nicht jeden Staat auf die Angemessenheit geprüft. Zudem kann nur ein schweizerisches Gericht verbindlich und abschliessend über die Anwendung von Art. 6 DSG entscheiden. Der Datenexporteur muss deshalb in diesem Fall die nötigen Rechtsabklärungen selbst vornehmen, z.B. durch Konsultation von Lehre und Rechtsprechung oder das Einholen von unabhängigen Rechtsgutachten.

[N03] Kein angemessener Schutz gemäss der Staatenliste des EDÖB oder Anzeichen, dass keine datenschutzkonforme Datenübertragung möglich ist (Art. 6 Abs. 2 lit. a DSG)

Fehlt der Staat als angemessen auf der Staatenliste des EDÖB oder bestehen trotz Vorhandenseins auf der Staatenliste konkrete Hinweise, wonach mit Blick auf den beabsichtigten Export nicht von einem angemessenen Datenschutzniveau ausgegangen werden kann, muss der Datenexporteur den Datenschutz mit hinreichenden Garantien, insbesondere durch einen Vertrag, sicherstellen. Grundlage werden in der Regel **Mustervertragsklauseln, sog. Standard Contract Clauses (SCC)** sein. Anzumerken ist, dass unternehmensinterne Datenschutzvorschriften, sog. **Binding Corporate Rules (BCR),** welche die Datenbekanntgabe ins Ausland innerhalb eines Konzerns oder zwischen verschiedenen Unternehmen unter einheitlicher Leitung regeln, von einem Datenexporteur im externen Verhältnis nicht als Ersatz von SCC verwendet werden können. BCRs sind ohne Zustimmung des externen Datenexporteurs und unabhängig von der Vertragslaufzeit meistens vom Datenimporteur individuell abänderbar und es fehlen zudem wesentliche Bestandteile, die in einem SCC abgebildet sind (z.B. Bestimmungen betreffend die Einsetzung von Subunternehmern).

[N04] Detaillierte Erfassung des Datentransfers

Eine detaillierte Erfassung des Datentransfers durch den Datenexporteur, z.B. mittels eines Verzeichnisses, ist die sachdienliche Basis für die Einschätzung des beabsichtigten Datenexports.

Es ist unter anderem Folgendes zu klären:

- Weisen die zu exportierenden Daten einen Personenbezug auf?
- Sind Personen bestimmt oder bestimmbar?
- Was ist der Zweck der Datenbekanntgabe?
- Welche Kategorien von Personendaten werden übermittelt?
- Gibt es weitere Auftrags- und Unterauftragsbearbeiter und befinden sich diese in Drittländern?
- Werden die Personendaten von Unternehmen bearbeitet, welche Rechtsordnungen in Drittländern unterstehen (z.B. US-amerikanische Cloudanbieter mit Servern in CH/EU/EWR)?
- Werden die Daten innerhalb des Drittlandes oder in ein weiteres Drittland weiterübermittelt oder gibt es Hinweise, dass es dazu kommen könnte?

[N05] Vier Garantien

Mit Blick auf behördliche Zugriffe im Drittland (z.B. zwecks nationaler Sicherheit oder Strafverfolgung) und die Rechte der Betroffenen hat der Datenexporteur zu prüfen, ob jene mit dem schweizerischen Datenschutzrecht und den schweizerischen Verfassungsgrundsätzen vereinbar sind. Er muss entsprechende Abklärungen selbst vornehmen und darf sich dabei nicht nur auf die Aussagen des Datenimporteurs verlassen. Dies kann er durch Konsultation von Literatur und Rechtsprechung oder das Einholen von unabhängigen Rechtsgutachten machen.

Folgende schweizerische Grundrechtsgarantien müssen im Drittland analog gewährleistet sein und es gilt zu prüfen, welche Mängel im Drittland vorliegen:

1. **Legalitätsprinzip: Klare, präzise und zugängliche Regeln (Art. 5 und Art. 164 BV)**
   Hinreichend bestimmte und klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden.

2. **Verhältnismässigkeit der Befugnisse und Massnahmen im Hinblick auf die verfolgten Regelungsziele (Art. 5 Abs. 2 BV und Art. 4 Abs. 2 DSG)**
   Die Befugnisse und Massnahmen der Behörden müssen geeignet und erforderlich sein, um die gesetzlichen Zwecke der behördlichen Zugriffe zu erfüllen. Zudem müssen sie für die Betroffenen zumutbar sein.

3. **Dem Einzelnen müssen wirksame Rechtsmittel zur Verfügung stehen (Art. 13 Abs. 2 BV zur Durchsetzung von Art. 15 DSG sowie Art. 8 EMRK)**
   Betroffene in der Schweiz müssen wirksame gesetzlich verankerte Rechtsbehelfe für die Durchsetzung ihrer Rechte zum Schutz der Privatsphäre und informationellen Selbstbestimmung (z.B. Auskunft-, Berichtigungs- und Löschungsrecht) haben.

4. **Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht (Art. 29 ff. BV und Art. 15 DSG)**
   Eingriffe in die Privatsphäre und informationelle Selbstbestimmung müssen einem wirksamen, unabhängigen und unparteiischen Kontrollsystem unterliegen (Gericht oder andere unabhängige Stelle, z. B. Verwaltungsbehörde oder parlamentarisches Gremium). Neben vorheriger (gerichtlichen) Genehmigung von Überwachungsmassnahmen (Schutz vor Willkür) muss auch die tatsächliche Funktionsweise des Überwachungssystems überprüft werden können.

Hinweis Anwendungsfall USA

Bestehen Anhaltspunkte, dass Personendaten in den USA direkt oder indirekt bearbeitet werden bzw. bearbeitet werden könnten, insbesondere bei Nutzung von Clouddiensten, kann der Fragebogen im Anhang für weitere Abklärungen verwendet werden [«*Datenschutzanfrage an Dienstleister/Anbieter mit möglichen direkten oder indirekten US-Beziehungen (mit Einbezug deren Subunternehmer unter weiteren Sub-Sub-Unternehmer und weiteren Dienstleistern/Anbietern)*»].

[N06] Analyse

Es ist eine Analyse des Datentransfers im Einzelfall und in Bezug auf das gewählte Instrument wie SCC sowie die rechtlichen Umstände im Drittland vorzunehmen. Der verantwortliche Datenexporteur muss bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen (z.B. Einholen von unabhängigen Rechtsgutachten).

In die Prüfung ist u.a. Folgendes miteinzubeziehen:

- Geltende Rechtsvorschriften im Zielland
- Praxis der Verwaltungsbehörden und Gerichtsbehörden
- Rechtsprechung

[N07] Garantien gewährleistet: SCC

Wenn die vier Garantien (vgl. N05) gewährleistet sind, kann mit standardmässigen SCC ein angemessenes Datenschutzniveau erreicht werden.

Es bleibt dann lediglich noch bei der individuellen Umsetzung der SCC zu berücksichtigen, ob sich eventuell weitere vertragliche Massnahmen zum individuellen Schutz (nicht gegen staatliche Zugriffe) aufdrängen. Solche Regelungen können z.B. folgende Bereiche miteinbeziehen:

- Betroffenenrechte stärken (z.B. Auskunftsrecht)
- Regelung von technischen Massnahmen als Bedingung für Datenübermittlungen vorsehen
- Befugnis des Datenexporteurs stärken, indem der Datenimporteur verpflichtet wird, sich bei den Datenbearbeitungssystemen Inspektionen zu unterziehen und Rechenschaft abzulegen
- Klauseln vorsehen, die bei Bedarf schnelles Verfahren der Datensicherung ermöglichen.

[N08] Garantien nicht gewährleistet: SCC und zwingend zusätzliche Massnahmen

Wenn die in N05 erwähnten Garantien im Drittland nicht umfassend gewährleistet sind, sind vorab in jedem Fall zusätzliche Massnahmen zu prüfen, die als „Ersatz“ für die fehlenden vier Garantien dienen.

Zusätzliche vertragliche Massnahmen (zwischen dem Datenexporteur und dem Datenimporteur) sind kaum möglich, weil sie drittstaatliche Behörden nicht binden können und dadurch behördliche Zugriffe nicht verhindern können. Beispielsweise sind auch Schadenersatzregelungen, die Zusicherung der Ergreifung von Rechtsbehelfen und Ausschöpfung von Rechtsmitteln gegen behördliche Anordnungen oder Transparenzberichte sind insbesondere dann ungenügend, wenn rechtliche Vorgaben im Drittstaat vorgehen bzw. diese vertraglichen Massnahmen durchkreuzen.

Die **zusätzlichen technischen und organisatorischen Massnahmen** müssen dergestalt sein, dass die Behördenzugriffe auf die übermittelten Personendaten im Zielland faktisch verhindert werden. Bei der Datenhaltung im Sinne eines reinen Cloud-Betriebs durch Dienstleister eines Staates ohne angemessenes Schutzniveau wäre z.B. eine Verschlüsselung denkbar, welche nach den Prinzipien BYOK («bring your own key») und zusätzlich BYOE («bring your own encryption») umgesetzt ist, so dass in der Cloud keine Klardaten vorliegen resp. in der Cloud keine Entschlüsselung und Verschlüsselung erfolgt. Bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland gestaltet sich der Einsatz solcher technischen Massnahmen indessen als anspruchsvoll.

Ergibt die Prüfung, dass das Fehlen einer oder mehrerer der vier Garantien gemäss N05 nicht durch zusätzliche Massnahmen ausgleichbar ist, muss nach N10 verfahren werden.

[N09] Übertragung der Daten

Nach Umsetzung der nötigen zusätzlichen Massnahmen muss der verantwortliche Datenexporteur regelmässig die sachlichen und rechtlichen Voraussetzungen überprüfen. Kommt er zum Schluss, dass die Datenschutzkonformität nicht mehr gegeben ist, ist nach N10 zu verfahren.

[N10] Aussetzung bzw. Beendigung der Datenbekanntgabe ins Ausland

Wenn mit zusätzlichen Massnahmen die festgestellten Mängel bezüglich der Erfüllung der vier Garantien nicht kompensiert werden können und damit keine hinreichende Garantie nach Art. 6 Abs. 2 lit. a DSG erreicht wird, ist der Datentransfer ins Ausland umgehend auszusetzen bzw. zu beendigen.

Anhang[1]

Datenschutzanfrage an Dienstleister/Anbieter mit möglichen direkten oder indirekten US-Beziehungen (mit Einbezug deren Subunternehmer unter weiteren Sub-Sub-unternehmer und weiteren Dienstleistern/Anbietern)

Dienstleister/Anbieter inkl. alle nachfolgenden Subunternehmer und beigezogene Dienstleister/Anbieter (auch von Software-Komponenten) nachfolgend «SIE»

Angesichts des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18, insbesondere jedoch nicht abschliessend der Absätze 138 bis 145, bitten wir dringend um Klärung der folgenden Fragen:

1 Direkte Anwendung von 50 U.S.C. § 1881a (= FISA 702)

1.1 Fallen SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten, die an SIE übermittelt werden, verarbeitet oder Zugang zu diesen Daten hat, unter eine der folgenden Definitionen in 50 U.S.C. § 1881(b)(4), die SIE oder die andere(n) Stelle(n) direkt unter 50 U.S.C. § 1881a (= FISA 702) fallen lassen könnte(n)?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

1.2 Insbesondere,

A. Sind SIE oder eine andere relevante US-Einheit ein Telekommunikationsunternehmen, wie dieser Begriff in Abschnitt 153 von Titel 47 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

B. Sind SIE oder eine andere relevante US-Einheit ein Anbieter von elektronischen Kommunikationsdiensten, wie dieser Begriff in Abschnitt 2510 von Titel 18 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

C. Sind SIE oder eine andere relevante US-Einheit ein Anbieter eines Ferncomputerdienstes, wie dieser Begriff in Abschnitt 2711 von Titel 18 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

[1] Der vorliegende Fragebogen wurde auf der Grundlage des Fragebogens von www.noyb.eu an die Schweiz angepasst und weiterentwickelt.

D. Sind SIE oder eine andere relevante US-Einheit ein anderer Anbieter von Kommunikationsdiensten, der Zugang zu drahtgebundener oder elektronischer Kommunikation hat, entweder wenn diese Kommunikation übertragen wird oder wenn diese Kommunikation gespeichert wird?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

E. Sind SIE oder eine andere relevante US-Einheit ein leitender Angestellter, Angestellter oder Vertreter einer Einheit, die unter die obigen Buchstaben (A), (B), (C), oder (D) fällt?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

2.1 Werden SIE von einer US-Muttergesellschaft oder einem US-Aktionär kontrolliert, oder haben SIE eine andere relevante Verbindung zu den USA, die das US-Recht indirekt gegen SIE durchsetzbar machen könnte?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

2.2 Wenn ja, sind SIE nach EU-Recht, nationalem Recht, Gesellschaftsrecht und internationalem Privatrecht verpflichtet, Anordnungen, Ersuchen oder Direktiven von US-Einrichtungen zu ignorieren, die von Ihnen verlangen würden, personenbezogene Daten, die SIE verarbeiten, der US-Regierung gemäss 50 U.S.C. § 1881a (= FISA 702) oder EO 12.333 offenzulegen, und sind SIE in der Lage, einen solchen Zugriff faktisch zu sperren?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

Bitte geben SIE an, auf welche rechtlichen und/oder technischen Schutzmassnahmen SIE sich berufen:

3 Verarbeitung unter EO 12.333

Arbeiten SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten verarbeitet, die von uns an SIE übermittelt werden, in irgendeiner Hinsicht mit den US-Behörden zusammen, die die Überwachung der Kommunikation gemäss EO 12.333 durchführen, sollte dies obligatorisch oder freiwillig sein?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

4 Andere anwendbare Gesetze

Unterliegen SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten verarbeitet, die von uns an SIE übermittelt werden, einem anderen Gesetz, das als Beeinträchtigung des Schutzes personenbezogener Daten nach der DSGVO (Artikel 44 DSGVO) oder von schweizerischem Recht angesehen werden könnte?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

wenn ja, geben SIE bitte diese Gesetze an:

5 Massnahmen gegen massenhafte und unterschiedslose Verarbeitung im Transitverkehr (FISA 702 und EO 12.333)

Weil auch der Gerichtshof im obengenannten Urteil die Notwendigkeit betont hat, sicherzustellen, dass personenbezogene Daten im Transit nicht der Massenüberwachung unterliegen, bitten wir um folgende Klarstellungen:

A. Haben SIE geeignete technische und organisatorische Massnahmen (siehe Artikel 32 DSGVO) für jeden Schritt der Verarbeitungsvorgänge getroffen, die sicherstellen, dass eine massenhafte und unterschiedslose Verarbeitung personenbezogener Daten durch oder im Auftrag von Behörden im Transitverkehr (z.B. im Rahmen des "Upstream"-Programms in den USA) unmöglich gemacht wird?

   ☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

B. Wenn ja, geben SIE bitte an, welche technischen und organisatorischen Massnahmen (einschliesslich Verschlüsselung) getroffen wurden, damit weder Inhalts- noch Metadaten von hochentwickelten staatlichen Akteuren mit direktem Zugang zum Internet-Backbone, zu Switches, Hubs, Kabeln und Ähnlichem verarbeitet werden können:

6 Beantwortung der oben gestellten Fragen

Wir bitten Sie, diese Fragen ohne unnötige Verzögerung zu beantworten, jedoch nicht später als fünf Arbeitstage ab Zugang dieses Fragebogens.

[Ort und Datum]

[Firma]

[rechtsgültige Unterzeichnung]