bitkom

Konzeptpapier BiTIAT

Konzeptpapier zum Bitkom Transfer Impact Assessment Tool (BiTIAT)

Konzept und Funktionsweise

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Rebekka Weiß, LL.M. | Leiterin Vertrauen & Sicherheit
T 030 27576-161 | r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenschutz

Lead-Autoren und Bearbeiter des BiTIAT
Achim Hubert (Sage), Alexander Hardinghaus (ReedSmith), Andrea Pawils (Telekom MMS), Andreas Splittgerber (ReedSmith), Ann-Kathrin Schaffer (Bosch), Arnd Böken (Graf von Westphalen Rechtsanwälte), Arne Senger (ReedSmith), Boris Nentwich (Infineon), Christoph Bausewein (Crowdstrike), Dirk Refflinghaus (Finanz Informatik), Dr. Falk Böhm (Olympus Corporation), Finjas Melvin Auricht (Telekom MMS), Frank Ingenrieth (SRIW), Heiko Gossen (migosens), Henrik von Kunhardt (Riscreen), Irina Michalowitz (Twilio), Jonas von Dall´Armi (Giesecke+Devrient), Judith Nink (SoSafe), Kathrin Steffens (init), Kerstin Harzendorf (T-Systems), Kristin Bock (scope & focus), Marc Schramm (Vodafone), Marianne Sieker (Transdev), Markus Stamm (Nokia), Martina Piaszczynski (Bayer), Nadia Schaff (Pinsent Masons), Percy Ott (Cisco), Petra Maid (Datev), Phillip Fischer (scope & focus), Rebekka Weis (Bitkom), Rene Schneider (DataGuard), Sabine Meinecke (Amazon), Sandra Scholz (DKB), Simone Böhm (Datev), Stefan Hessel (Reusch Rechtsanwaltsgesellschaft), Stephan Rehfeld (scope & focus), Volker Schwarzhaupt (E.ON), Waldemar Grudzien (Core), Željko Matas (Brystol-Myers Squibb)

Layout

Lea Joisten

Inhalt

1 Hintergründe zur Notwendigkeit einer systematischen Prüfung von Drittstaatentransfers

Die mit dem Urteil des Europäischen Gerichtshof (»EuGH«) vom 16. Juli 2020, Az. C-311/18 (»Schrems II-Urteil«) herbeigeführte Rechtslage hat lange Zeit für Ratlosigkeit und Unsicherheit innerhalb der Industrie zum Umgang mit internationalen Datentransfers geführt. Die Unsicherheit betrifft weniger den unmittelbar umsetzbaren Aspekt der Unwirksamkeit des Angemessenheitsbeschlusses zum Privacy Shield. Sie betrifft vielmehr die subtileren Konsequenzen für internationale Datentransfers generell. Denn nach Maßgabe des Urteils bestehen selbst im Falle der Verwendung von Standardvertragsklauseln im Sinne von Art. 46 Abs. 2 lit. d) DSGVO weitergehende Prüfanforderungen sowohl seitens der Unternehmen als auch seitens der Aufsichtsbehörden zur Frage der Notwendigkeit zusätzlicher Maßnahmen zugunsten des Schutzes der Rechte und Freiheiten von Betroffenen bei Drittstaatentransfers.

Zu den sich anschließenden Fragen zu den Auslösern für die Notwendigkeit zusätzlicher Maßnahmen sowie zu der Art der Maßnahmen selbst trifft der EuGH keine klaren Aussagen, sodass dieses Vakuum durch die Praxis zu füllen ist.

Das bestehende Vakuum ist aus Sicht der von Bitkom repräsentierten Mitgliedsunternehmen nicht akzeptabel, denn es fehlt an Rechts- und Planungssicherheit. Über alle Industriebereiche und unternehmensinterne Prozesse hinweg hat sich seit Jahren eine Praxis etabliert und im Vertrauen auf die bestehende Rechtlage auch verfestigt. Diese Praxis sieht sich unter Umständen Veränderungen gegenüber, die als Folge einer undifferenzierten Umsetzung des Schrems II-Urteils disruptive Folgen haben können. Diese Bedenken haben in den vergangenen Monaten keinerlei Widerhall gefunden. Weder der Europäische Datenschutzausschuss noch die deutschen Aufsichtsbehörden haben hierzu bislang überzeugende Konzepte vorlegt. Das gilt sowohl für die unmittelbar nach Urteilsfällung herausgegebenen FAQs als auch für entsprechende Pressemitteilungen. Deshalb hat sich Bitkom seit August 2020 dieser Herausforderung im Rahmen einer Arbeitsgruppe angenommen und dabei ein Konzept zur strukturierten Prüfung sowie ein unterstützendes Tool entwickelt.

1.1 Erläuterung zum Tool und Bezug zu SCCs

Das Prüfkonzept und das Bitkom Transfer Impact Assessment Tool (BiTIAT) erlauben die Prüfung von Datentransfers in (zunächst) 5 wichtige Transferländer. Die Funktionsweisen des Tools sind in den nachfolgenden Kapiteln beschrieben.

Die Übermittlung von personenbezogenen Daten basierend auf den EU-Standarddatenschutzklauseln (auch Standardvertragsklauseln, Standard Contractual Clauses, SCC) erfordert nach Klausel 14 eine Beurteilung der besonderen Umstände der Übermittlung sowie der relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes. Diese Prüfung wird auch Transfer Impact Assessment (TIA) genannt.

Der Arbeitskreis Datenschutz des Bitkom hat seine Expertise in einer Systematik zur Unterstützung eines solchen TIA gebündelt und in ein Tool (das BiTIAT) überführt.

Das BiTIAT nimmt den Nutzern die Pflichten als Verantwortliche/Verantwortlicher und Datenexporteur nicht ab, sondern bietet ein strukturiertes Rahmenwerk für die Bewertung und Dokumentation. Es stellt keine Rechtsberatung dar. Im Falle von Unsicherheiten bei der Dateneingabe ist ggf. fachlich qualifizierte Hilfe in Anspruch zu nehmen. Das gilt auch bei der Entscheidung über die Anwendung zusätzlicher Maßnahmen.

Der finale Report des BiTIAT kann als Word-Datei exportiert werden und ggf. auch weiter angepasst werden. Er kann so auch zum Bestandteil weiterer Dokumentationen werden.

1.2 Voraussetzungen

Das Tool bewertet ausschließlich zusätzliche Gefährdungen, die sich aus dem Umstand der Übermittlung von personenbezogenen Daten in ein unsicheres Drittland ergeben. Daher müssen Sie die grundsätzliche Zulässigkeit der Verarbeitung sowie die allgemein notwendigen technischen und organisatorischen Maßnahmen vorher feststellen.

Ferner wird der Abschluss von aktuell gültigen Standarddatenschutzklauseln vorausgesetzt.

Zur Nutzung des Tools müssen die Nutzer über ein Mindestmaß an Kenntnissen über die Datenübermittlung verfügen. Das schließt insbesondere Informationen zur Herkunft und zum Schutzbedarf der Daten sowie zur weiteren Verarbeitungskette ein. Natürlich muss auch das betreffende Drittland bekannt sein.

Bei der Auswahl von Maßnahmen aus dem Maßnahmenprofil bedarf es Kenntnisse und Expertise über die Umsetzbarkeit von Maßnahmen im konkreten Szenario.

1.3 Funktionsweise

Das BiTIAT bietet einen Rahmen für die Durchführung der Transfer-Impact-Assessments und stellt zudem die erforderliche Dokumentation bereit. Es standardisiert die Analyse des Drittlands und des jeweiligen Datentransfers. Die Software schlägt zudem zusätzliche Schutzmaßnahmen vor. Mögliche Gefährdungen für relevante Datenschutzziele der DS-GVO verknüpfen die genannten Komponenten. Die Modellierung dieser Gefährdungen ist zentraler Baustein der bereitgestellten Standardisierung und Automatisierung.

Von den Nutzern eingegebene Daten wirken als Eingangsgrößen für die Ermittlung von möglichen Gefährdungen für die Freiheiten und Rechte der Betroffenen, die Gewährleistungsziele. Diese Gefährdungen werden zunächst in Echtzeit für den Datenübermittlungsvorgang berechnet (»Übermittlungsprofil«). Für einige Länder wurden bereits Analysen nach den Maßgaben der Standarddatenschutzklauseln durchgeführt. Hieraus wurden ebenfalls Gefährdungen für die Gewährleistungsziele ermittelt (das sogenannte »Drittlandsprofil«).

Das Tool verknüpft im Hintergrund das Übermittlungs- und das Drittlandsprofil. Es entsteht ein Gefährdungsprofil für die konkrete Übermittlung.

In der Software sind Schutzmaßnahmen verschiedener Kategorien hinterlegt (organisatorisch, technisch, vertraglich). Die Zuordnung der einzelnen Maßnahmen zu einzelnen Gefährdungen ist statisch vorbestimmt. Das BiTIAT stellt sie aber in Abhängigkeit vom Gefährdungsprofil dynamisch zusammen (»Maßnahmenprofil«). Das Maßnahmenprofil ist die Arbeitsgrundlage für Ihre Bewertungen und Entscheidungen.

Das BiTIAT beruht also neben den statischen Festlegungen vor allem auf der Dateneingabe der Nutzer.

2 Details zur Funktionsweise

2.1 Dokumentation über die Notwendigkeit und Wirksamkeit zusätzlicher Maßnahmen

Das Bitkom-TIA-Tool liefert ein für den jeweiligen Nutzer unmittelbar verwendbares Ergebnis. Ein solches Ergebnis liegt darin, dass eine fundierte und auf objektiven Kriterien beruhende Aussage zur Notwendigkeit zusätzlicher Maßnahmen getroffen wird und entsprechende konkrete Maßnahmen dokumentiert werden können. Deshalb liefert das Bitkom Tool einen Report, der die Adäquanz des relevanten Drittlands im Hinblick auf das dort implementierte Datenschutzniveau mit den konkreten Umständen der Datenübermittlung zusammenführt. Auf der Grundlage dieser Zusammenschau wird ein Maßnahmenkatalog vorgeschlagen, der vom jeweiligen Nutzer individuell kommentiert und ggf. auch um weitere Maßnahmen ergänzt werden kann.

Die Entscheidung über die Auswahl konkret zu treffender Maßnahmen liegt ausschließlich beim jeweiligen Nutzer bzw. bei dem betroffenen Datenexporteur. Insoweit bietet das Bitkom-Tool neben den genannten inhaltlichen Features zur Ermittlung und Steuerung der Compliance der Datenübermittlung an sich auch den Rahmen zur Umsetzung der Rechenschaftsanforderungen.

Ausgangspunkt des Prüftools und der Prüfschritte ist stets der jeweilige Datentransfer. Nutzer des Tools müssen daher neben bereits vorhandenen Schutzmaßnahmen auch den jeweiligen Datentransfer beschreiben (können).

Folgende Fragen sind hierfür relevant:

1. Bestehen besondere Anforderungen an die Vertraulichkeit?
2. Sind die betroffenen Daten ausschließlich aus öffentlichen Quellen erhoben?
3. Liegt eine wirksame Einwilligung aller Betroffenen zur Übermittlung dieser Daten vor?
4. Erfolgt eine persistente Speicherung der Daten im Drittland?
5. Erfolgt die Übermittlung ausschließlich in Form eines Remote-Zugriffes aus dem Drittland heraus auf Systeme im EWR, ohne dass eine Speicherung im Drittland vorgesehen ist?
6. Erfolgt die Übermittlung rein konzernintern?
7. Werden oder sollen die Daten innerhalb des Drittlandes an Dritte/weitere Empfänger übermittelt werden?

2.2 Bedrohungsbasierte Steuerung von Maßnahmen

Die zusätzlichen Maßnahmen werden im Bitkom-Tool über ein Mapping auf die tatsächlichen Bedrohungen basierend auf den Umständen der Übermittlung sowie der rechtlichen Situation im Drittland gesteuert. Die Bedrohungen spiegeln sich in einer Auswahl der Datenschutz-Gewährleistungsziele des Standard-Datenschutzmodells wider, die im Kontext der Datenübermittlung in ein Drittland relevant sein können. Es handelt sich dabei um Vertraulichkeit, Verfügbarkeit, Integrität, Transparenz und Intervenierbarkeit.

Diese Datenschutz-Gewährleistungsziele lassen sich sämtlich auf Normen der DSGVO beziehen und bilden damit in aggregierter Form das im Rahmen der Art. 44 ff. DSGVO relevante Gesetzesprogramm ab. Durch die implementierte Logik werden Maßnahmen vorgeschlagen, die geeignet sind, solche Bedrohungen zu behandeln bzw. diesen entgegen zu wirken. Dabei können Maßnahmen prozeduraler, technischer oder vertraglicher Art sein und ihrerseits direkt oder indirekt wirken. Das Mapping der Maßnahmen auf die konkreten Bedrohungen für die Gewährleistungsziele sowie die Beurteilung ihrer Wirksamkeit erfolgte manuell in einem ausführlichen und durch ein 4-Augen-Prinzip abgesichertes Verfahren.

> Es sind 5 relevante Zielländer im BiTIAT enthalten.

3 Profilbasierte Identifikation von Bedrohungen für die Datenschutz-Gewährleistungsziele

Ob die Datenübermittlung in ein Drittland tatsächlich mit Bedrohungen für die genannten Gewährleistungsziele verbunden ist, wird durch die Verbindung eines Übermittlungsprofils mit einem Drittlandsprofil ermittelt.

Für die Prüfung relevante Profile

- Drittlandsprofil
- Übermittlungsprofil
- Bedrohungsprofil
- Maßnahmenprofil

3.1 Drittlandsprofil

Für die Erstellung des Drittlandsprofils werden innerhalb von 6 Prüfdomänen insgesamt 25 Einzelparameter des Datenschutzniveaus im Drittland geprüft.

Prüfdomänen:

1. Bestehen legale Restriktionen für Privacy by design, Privacy by default oder die Datensicherheit im Drittland?
2. Fällt der gesetzliche Rahmen für (präventive, repressive, strategische) Zugriffe auf personenbezogene Daten durch Hoheitsträger in Hinblick auf: (i) Regelungsdichte (ii) Formale Anforderungen (iii) materielle Anforderungen hinter das EU-Niveau zurück?
3. Besteht eine relevante eingeschränkte Möglichkeit der nachträglichen Information von Zugriffen an Exporteur oder Betroffenen?
4. Besteht eine relevante eingeschränkte Möglichkeit der nachträglichen Überprüfung von Zugriffen auf Rechtmäßigkeit zugunsten von Betroffenen?

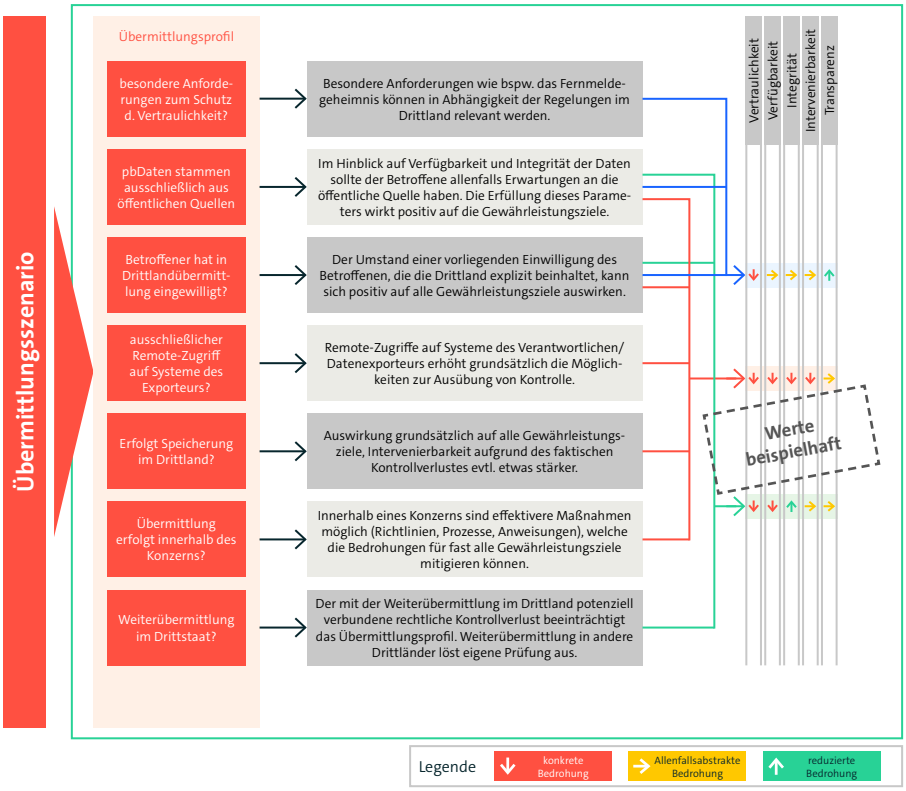
5. Es existiert kein allgemeines Bekenntnis zum Grundrechtsschutz im Drittland (bezogen auf datenschutzrelevante Grundrechte)? = Generelle Rechtsstaatlichkeitsprüfung

6. Eine effektive Rechtsdurchsetzung im Drittland (Unabhängigkeit der Gerichte, keine faktischen Rechtsweghindernisse) ist nicht sichergestellt? = effektiver gerichtlicher Rechtsschutz

Diese Prüfung erfolgt daraufhin, ob der jeweilige Parameter, der für die Adäquanz des Datenschutzniveaus für relevant gehalten wird, im betreffenden Drittland durch das dort vorhandene Rechtsregime ebenfalls implementiert oder aber unterlaufen wird. Auf der Ebene der jeweiligen Prüfdomäne wird von Adäquanz ausgegangen, wenn mindestes 75 Prozent der Einzelparameter dieser Domäne im Drittland implementiert sind. Insofern wird keine Aussage über das Rechtssystem schlechthin getroffen, sondern relevant ist allein die Aussage auf Ebene der Prüfdomäne. Jede Prüfdomäne wird wiederum auf eines oder mehr der o. g. Gewährleistungsziele gemappt. Je nach ermittelter Adäquanz kann damit eine abstrakte Aussage getroffen werden, ob Datenschutz-Gewährleistungsziele durch das im Drittland implementierte Rechtsregime unter Druck geraten können oder nicht. In diesem Falle werden diese Gewährleistungsziele auf der Ebene des Drittlandsprofils »aktiviert«. Muss also etwa die Frage »Bestehen legale Restriktionen für Privacy by design, Privacy by default oder die Datensicherheit im Drittland?« mit »ja« beantwortet werden, werden die Gewährleistungsziele Vertraulichkeit und Integrität »aktiviert«. Ob sich jedoch hieraus eine tatsächliche Bedrohung für diese beiden Gewährleistungsziele ableiten lässt, ergibt sich nach der Betrachtung der konkreten Umstände der Übermittlung.

3.2 Übermittlungsprofil

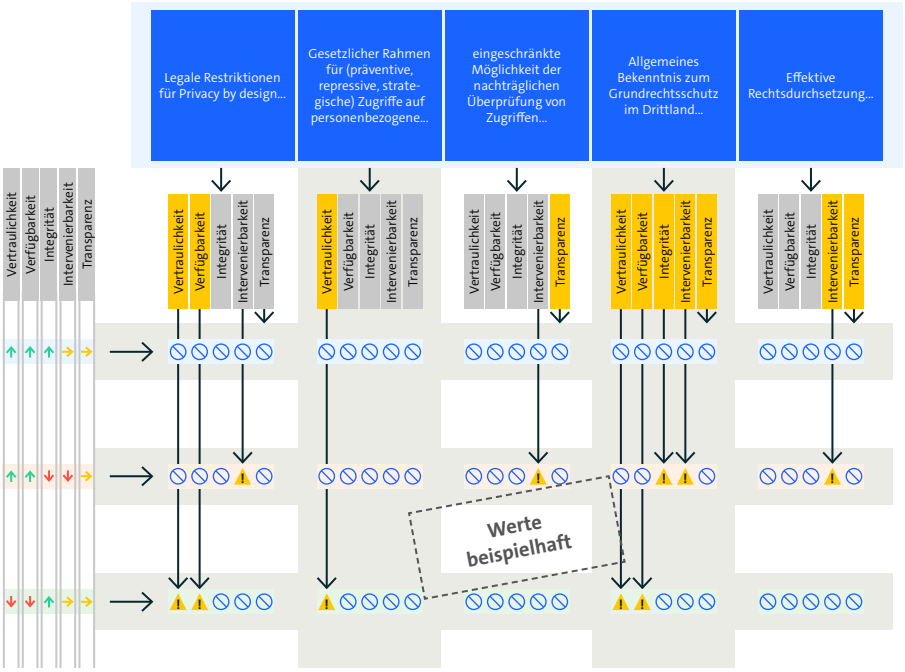
Für die Erstellung des Übermittlungsprofils werden die wesentlichen Aspekte der Datenübermittlung geprüft. Dabei wird auf diejenigen Aspekte abgestellt, welche aus der Perspektive eines Betroffenen Treiber für die Exposition der personenbezogenen Daten im Drittland sind (Datentransfer vs. Datenzugriff, Weitergabe außerhalb vs. innerhalb des Unternehmens, Einwilligung vs. anderer Erlaubnistatbestand, Einfachübermittlung vs. Übermittlungskette, öffentliche vs. nicht-öffentliche Quellen). Jede dieser Übermittlungsparameter wird wiederum auf eine oder mehrere der o. g. Gewährleistungsziele gemappt. Je nach Ausprägung der einzelnen Übermittlungsparameter ergibt sich ein Übermittlungsprofil. Aufgrund der unterschiedlichen Wirkung einzelner Parameter (teils begünstigend, teils konträr zu möglichen Bedrohungen), erfolgt eine Konsolidierung auf 3 Parameter für die weitere Analyse: Beispielsweise wird der verschärfende Umstand, dass es sich Daten mit besonderen Anforderungen an die Vertraulichkeit handelt (bspw. Daten des Fernmeldegeheimnisses) dadurch wieder aufgehoben, wenn der Betroffene in die Übermittlung eingewilligt hat.



Abhängig von der Ausprägung dieser Parameter ist die Exposition der personenbezogenen Daten stärker oder schwächer ausgeprägt und kann eine individuelle Aussage getroffen werden, ob Datenschutz-Gewährleistungsziele durch die Übermittlung (in ein Drittland) unter Druck geraten können. In diesem Falle werden die entsprechenden Bedrohungen auf der Ebene des Übermittlungsprofils »aktiviert«.

3.3 Bedrohungsprofil

Wenn und soweit Bedrohungen für Datenschutz-Gewährleistungsziele sowohl auf der Ebene des Übermittlungsprofils als auch auf der Ebene des Drittlandsprofils »aktiviert« werden, wandeln sich die für sich genommen abstrakten Bedrohungen für die Datenschutz-Gewährleistungsziele in ein konkretes Bedrohungsprofil. Denn vor dem Hintergrund des Drittlandsprofils bestehen (abstrakte) rechtliche Risiken für den Betroffenen, die sich auf Grund des konkreten Übermittlungsvorgangs auch tatsächlich konkretisieren können. In einem solchen Fall müssen die ermittelten Risiken mit zusätzlichen Maßnahmen adressiert werden. Diesen (konkreten oder abstrakten) Bedrohungen sind verschiedene Maßnahmen zugeordnet, die grundsätzlich zur Mitigation der Bedrohungen geeignet sein können.



3.4 Maßnahmenprofil

Das so ermittelte Maßnahmenprofil enthält eine Liste aller hinterlegter Maßnahmen, die basierend auf den konkreten oder abstrakten Bedrohungen im Drittland als Gegenmaßnahme helfen können. Dabei erfolgt eine Gewichtung der Maßnahmen anhand eines Relevanzwertes. Abhängig von der Häufigkeit, mit der die Maßnahme basierend auf den ermittelten Bedrohungen (als Ergebnis der Schnittpunkte zwischen Übermittlungs- und Drittlandparameter) ausgelöst wurde, sowie der Wirkungsart (direkt oder indirekt), errechnet sich die Relevanz. Das heißt, dass je häufiger eine Maßnahme als mögliche Maßnahme identifiziert wurde, desto höher die Relevanz. Direkt wirkende Maßnahmen werden gegenüber den indirekt wirkenden Maßnahmen zusätzlich mit dem Faktor 100 multipliziert.

»Direkte Wirkung« bedeutet, dass die Bedrohung durch die Maßnahme sich direkt reduzieren oder eliminieren lässt, eine »indirekte Wirkung« hat eine begünstigende Wirkung zur Reduzierung der Eintrittswahrscheinlichkeit oder der Schadensauswirkung, sollte sich eine Bedrohung realisieren.

4 Abschließende Bewertung

4.1 Faktoren zur Bewertung

Alle ermittelten Maßnahmen wirken auf die Bedrohungen für die jeweiligen Gewährleistungsziele, die im Hintergrund das Fundament der Bedrohungsanalyse bilden. Dies geschieht ungeachtet weiterer Details, die ggf. Einfluss auf eine abschließende Bewertung der Erforderlichkeit bestimmter Maßnahmen haben können. Solche weichen Faktoren können beispielsweise

- die Anzahl oder die Kategorie von Betroffenen sein,
- die Sphäre, aus der die Daten stammen,
- Anzahl der Datensätze,
- ob es sich um strukturierte oder unstrukturierte Daten handelt,
- die Branche und Relevanz des Empfängers im Drittland,
- die angewandte Praxis von Befugnissen der Behörden im Drittland.

Daher ist der Sanity-Check, also eine finale Bewertung basierend auf allen Details der Umstände einer Übermittlung abschließend notwendig. Diese Bewertung obliegt dem Verantwortlichen und muss mit einer Entscheidung abschließen, ob die gewählten Maßnahmen ausreichend sind, um die eventuellen Bedrohungen im Drittland ausreichend zu mitigieren.

Maßnahmenrelevanz:	110
Nummern	P.002
Bezeichnung	Risikobewertung durch Anbieter
Wirkung:	indirekt
Erläuterung Wirksamkeit:	Maßnahme liefert keine Hinweise auf konkrete Zugriffe bestimmter Daten. Daher kann Maßnahme nur zur Bewertung der Eintrittswahrscheinlichkeit eines Zugriffs dienen (entweder vor erstmaliger Übermittlung oder im Rahmen der lfd. Zusammenarbeit).

☒ Maßnahme wird nicht angewandt

Begründung:

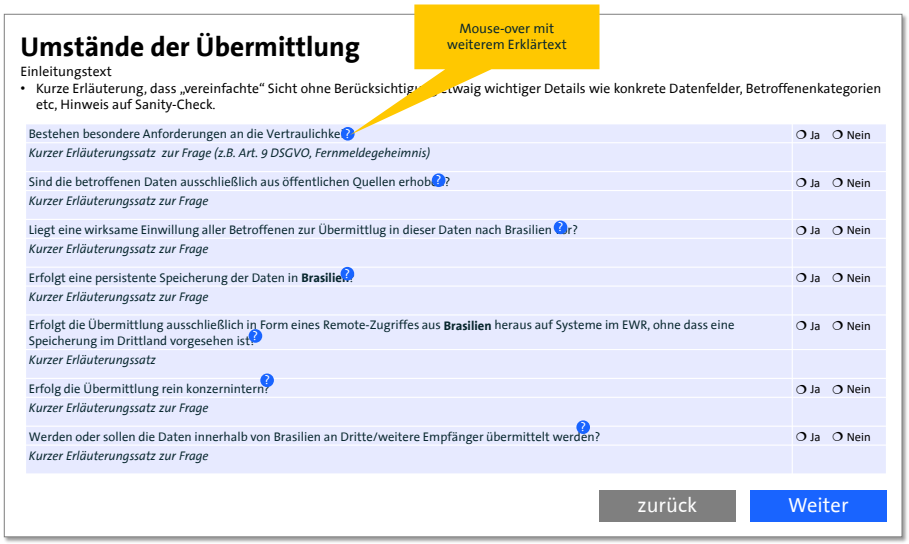
Die Maßnahme ist angesichts der Kritikalität der Daten und der Bedrohungslage im Drittland nach eingehender Betrachtung als nicht erforderlich bewertet worden. Ein adäquates Schutzniveau für die Rechte und Freiheiten der Betroffenen kann mit den verbleibenden Maßnahmen erreicht werden.

4.2 TIA Tool Benutzeransicht

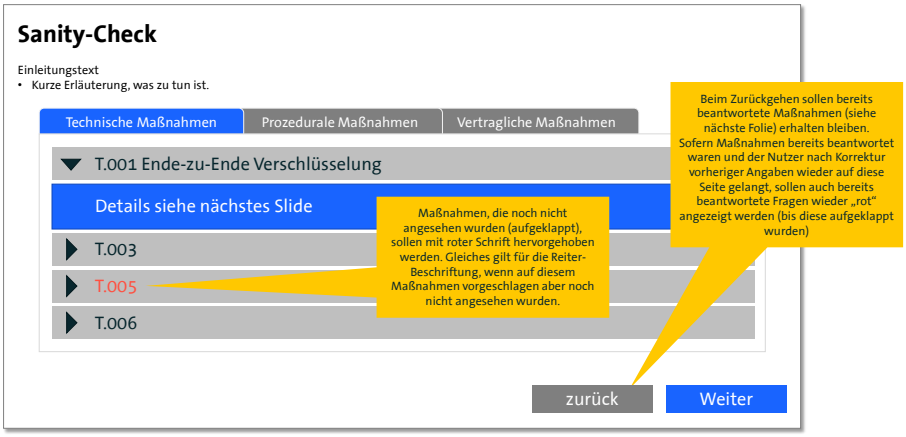
Startseite BiTIA Tool

1. Eingabeseite

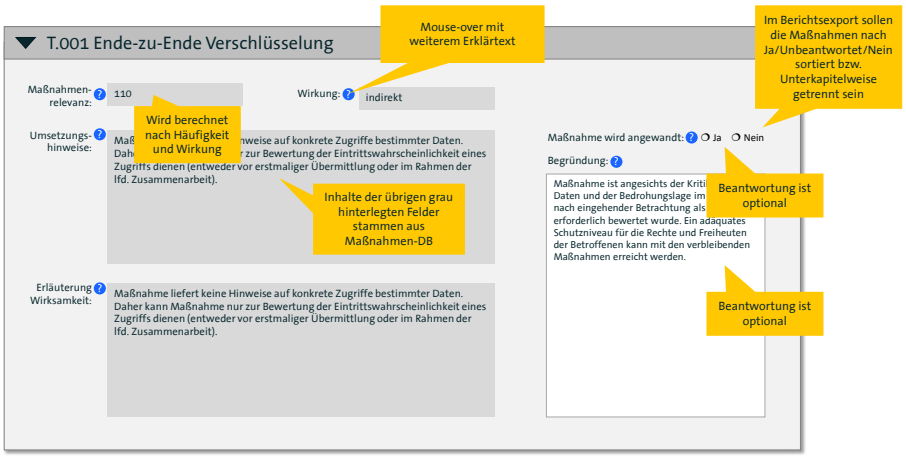
2. Eingabeseite



3. Eingabeseite



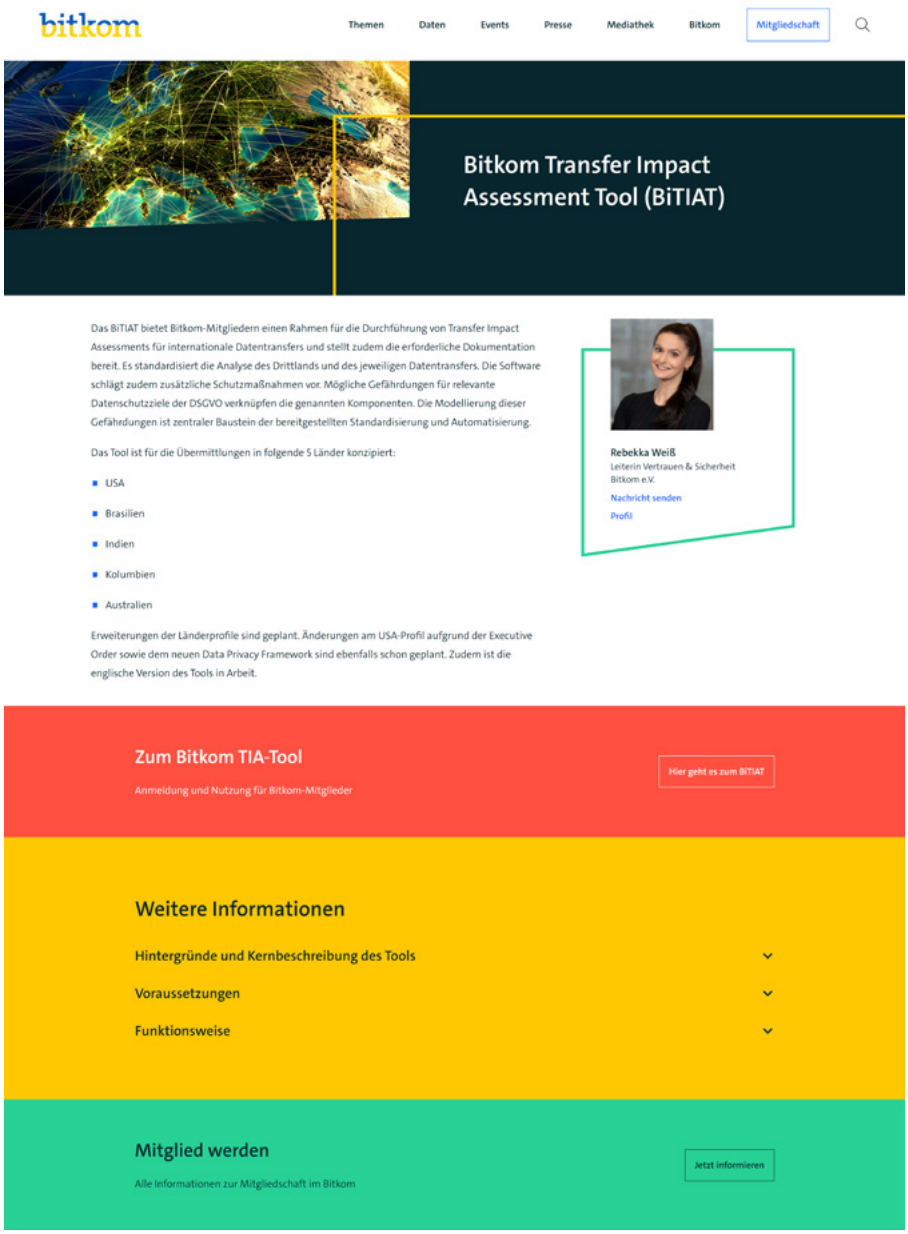
Details 3. Eingabeseite (Sanity-Check)



4. Eingabeseite

5 Zugang zum BiTIAT und weitere Hinweise

Das Bitkom Transfer Impact Assessment Tool (BiTIAT) ist für Bitkom-Mitglieder[1] über unsere ↗ Webseite zugänglich. Das BiTIAT wird inhaltlich nach und nach um weitere Länderprofile ergänzt. Auch eine englischsprachige Fassung soll in 2023 zugänglich gemacht werden.



1 Noch kein Bitkom-Mitglied? Hier gibt es Hinweise zur Mitgliedschaft: ↗ https://www.bitkom.org/Bitkom/Mitgliedschaft/Mitglied-werden/index.jsp

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org