Datenverarbeitung in einem Drittland: Data Transfer Impact Assessment (TIA) – eine Einführung ins Thema

Erarbeitet von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Version 1.0

Stand der Bearbeitung: 10. April 2023

Autoren (Nennung in alphabetischer Reihenfolge)

Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security Solutions GmbH
Regina Mühlich	AdOrga Solutions GmbH

Haftungsausschluss

- Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.
- Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.
- Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Inhaltsverzeichnis

1 Einleitung

Als Drittland, oftmals auch Drittstaat genannt, werden aus europäischer Sicht alle Staaten bezeichnet, welche nicht zum Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) gehören. Wenn unter Geltung der Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten in einem oder mehreren Drittländern verarbeitet werden, muss gemäß Art. 44 S. 1 DS-GVO zwingend allen in Kap. V DS-GVO enthaltenen Bedingungen genügt werden, aber gleichermaßen auch alle anderen Vorgaben der DS-GVO eingehalten werden. Es ist dabei unerheblich, ob die personenbezogenen Daten von einem innerhalb der EU befindlichen bzw. agierenden Verantwortlichen oder Auftragsverarbeiter einem anderen Verantwortlichen, einem anderen Auftragsverarbeiter oder sonstigen Dritten (wie z. B. einer staatlichen Behörde) in einem Drittland zur Kenntnisnahme oder Verarbeitung bereitgestellt werden. Die Vorgaben der DS-GVO müssen uneingeschränkt gewährleistet werden.

Liegt kein Art. 45 DS-GVO genügender Angemessenheitsbeschluss der EU-Kommission vor, dürfen entsprechend den Vorgaben von Art. 46 Abs. 1 DS-GVO Verantwortliche oder Auftragsverarbeiter nur Daten in einem Drittland oder von einer internationalen Organisation verarbeiten lassen, wenn

a) geeignete Garantien vorgesehen sind, welche sicherstellen, dass das von der DS-GVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird, sowie
b) durchsetzbare Rechte und wirksame Rechtsbehelfe für betroffene Personen zur Verfügung stehen.

Die Beurteilung, ob diese Vorgaben erfüllt sind oder nicht, wird häufig als „Data Transfer Impact Assessment“ (DTIA) oder kürzer als „Transfer Impact Assessment“ (TIA) bezeichnet. Im Folgenden wird dargestellt, worauf bei einer TIA zu achten ist und wie bei einer TIA vorgegangen werden kann. Hierzu werden einerseits die von der EU-Kommission bereitgestellten Instrumente aus Kap. V DS-GVO betrachtet, die ihrerseits Einfluss auf die Anforderungen an eine TIA aufweisen, andererseits das Urteil des EuGH in der Sache Schrems II, aus welchem ebenfalls zu beachtende Anforderungen, die in einer TIA geprüft werden müssen, erwachsen.

2 Von der EU-Kommission bereitgestellte Instrumente für Drittland-Verarbeitung: Angemessenheitsbeschluss und Standarddatenschutzklauseln

2.1 Angemessenheitsbeschluss nach Art. 45 DS-GVO

Entsprechend Art. 45 DS-GVO kann die EU-Kommission

- einem Drittland,
- einem Gebiet in einem Drittland,
- für ein oder mehrere spezifische Sektoren einem Drittland oder
- für internationale Organisation

ein angemessenes Schutzniveau attestieren. Dies erfolgt über einen Angemessenheitsbeschluss, wobei die EU-Kommission eine Prüfung entsprechend den Vorgaben von Art. 45 Abs. 2 DS-GVO durchführen muss. D. h. speziell bei einem Angemessenheitsbeschluss ist für Verantwortliche oder Auftragsverarbeiter keine Prüfung, abgesehen von der regelhaften Prüfung im Rahmen der Anforderungen von Art. 28 DS-GVO, mehr erforderlich (aber immer noch möglich), da die Prüfung bereits durch die EU-Kommission erfolgte.

Der Durchführungsrechtsakt eines Angemessenheitsbeschlusses darf dabei nur entsprechend den Vorgaben Art. 93 Abs. 2 DS-GVO erfolgen, worin auf Art. 5 der Verordnung (EU) 182/2011[1] verwiesen wird. Das in Art. 5 der Verordnung (EU) 182/2011 beschriebene Prüfverfahren beruht auf Art. 291 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)[2], d. h. EU-Mitgliedstaaten bekommen dadurch die Möglichkeit, Durchführungsbefugnisse durch die Kommission zu kontrollieren. Hierdurch besitzen die EU-Mitgliedsstaaten auch bzgl. eines Angemessenheitsbeschlusses der EU-Kommission eine Kontrollmöglichkeit, denn nach Art. 5 Abs. 4 lit. c Verordnung (EU) 182/2011 können die Mitglieder des Ausschusses, also Vertreter der Mitgliedstaaten, einen Angemessenheitsbeschluss mit einfacher Mehrheit auch ablehnen.

Das EU-Parlament selbst hat hingegen keine Möglichkeit, einen Angemessenheitsbeschluss abzulehnen. Nach Art. 11 Verordnung (EU) 182/2011 kann das EU-Parlament die EU-Kommission lediglich darauf hinweisen, dass der Entwurf eines Angemessenheitsbeschlusses nach Ansicht des EU-Parlaments die in der DS-GVO enthaltenen Durchführungsbefugnisse der EU-Kommission überschreitet.

Allerdings urteilte der EuGH[3] schon 2015, dass eine nationale Datenschutzaufsichtsbehörde eigene Ermittlungen bzgl. des Schutzniveaus anstellen muss, falls bei der Aufsichtsbehörde eine Beschwerde eingeht. Kommt die Aufsichtsbehörde bei der Prüfung zu dem Ergebnis, dass in dem Drittland kein angemessenes Datenschutzniveau vorhanden ist, muss die Aufsichtsbehörde entsprechend § 21 Abs. 1 BDSG ein Verfahren vor dem Bundesverwaltungsgericht beginnen.

---

[1] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren. Online, zitiert am 2023-04-08; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32011R0182

[2] Vertrags über die Arbeitsweise der Europäischen Union. Online, zitiert am 2023-04-08; verfügbar unter http://data.europa.eu/eli/treaty/tfeu_2012/oj

[3] EuGH, Urt. v. 2015-10-06, AZ C-362/14 („Schrems-I"), insbesondere Rn. 57 „[…] müssen die nationalen Kontrollstellen daher, wenn sich eine Person mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie wendet, in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung dieser Daten die in der Richtlinie aufgestellten Anforderungen gewahrt werden." Online, zitiert am 2023-04-08; verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

Die EU-Kommission veröffentlicht die Liste der Drittländer, für die ein Angemessenheitsbeschluss vorliegt, auf ihrer Internetpräsenz.[4]

2.2 Standarddatenschutzklauseln entsprechend Art. 46 DS-GVO

Entsprechend Art. 46 Abs. 2 lit. c DS-GVO kann die EU-Kommission Standarddatenschutzklauseln erlassen, wobei auch hier ein Prüfverfahren nach Art. 93 Abs. 2 Verordnung (EU) 182/2011 durchgeführt werden muss. D. h. auch bei den von der EU-Kommission erlassenen Standarddatenschutzklauseln besteht eine Kontrollmöglichkeit durch die EU-Mitgliedstaaten.

Die EU-Kommission erließ 2021 Standarddatenschutzklauseln[5], nannte diese jedoch entgegen den Vorgaben der DS-GVO „Standardvertragsklauseln" (engl. „standard contractual clauses", daher häufig durch „SCC" abgekürzt). Basiert eine Verarbeitung personenbezogener Daten auf den von der EU-Kommission veröffentlichten Standarddatenschutzklauseln, so fordert auch Klausel 14[6] dieser Standarddatenschutzklauseln, die für alle Module zwingend anzuwenden ist, eine Prüfung der Rechtsvorschriften und Gepflogenheiten im Drittland, die sich auf die Einhaltung der Klauseln auswirken könnten - folglich die Durchführung einer TIA.

In Klausel 14 finden sich mehrere Anforderungen:

- Sowohl Datenexporteur als auch Datenimporteur verpflichten sich per Vertrag, dass keine Partei einen Grund zur Annahme hat, dass im Drittland geltenden Rechtsvorschriften und Gepflogenheiten, „einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten", im Widerspruch mit den Regelungen des Vertrages stehen (Klausel 14 lit. a).
    - Die Formulierung „keine Partei einen Grund zur Annahme hat" beinhaltet die Pflicht, sowohl für den Datenexporteur als auch den Datenimporteur, sorgfältig zu prüfen, ob nach objektiven Maßstäben keine Tatsachen existieren, die eine andere Annahme nahelegt.
    - Prüfgegenstand sind neben den im Drittland geltenden Rechtsvorschriften auch „Gepflogenheiten" im Drittland. Die EU-Kommission beschreibt in den Erwägungsgründen nicht, was unter „Gepflogenheiten" zu verstehen ist. In der Literatur wird unter „Gepflogenheiten" mehrheitlich die Anwendung und Durchsetzung der Rechtsvorschriften im Drittland verstanden,[7] also z. B. ob Datenschutzverstöße geahndet werden.
- Insbesondere bewerteten die Parteien (Klausel 14 lit. b)
    - die besonderen Umstände der Übermittlung, einschließlich
        - der Länge der Verarbeitungskette,
        - der Anzahl der beteiligten Akteure,
        - der verwendeten Übertragungskanäle,
        - beabsichtigte Datenweiterleitungen,

[4] EU-Kommission: Adequacy decisions. Online, zitiert am 2023-04-08; verfügbar unter https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[5] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Online, zitiert am 2023-04-08; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX:32021D0914

[6] Bei der Interpretation von Klausel 14 sollten insbesondere auch ErwGr. 18, 19, 20 und 21 der Standarddatenschutzklauseln mitberücksichtigt werden

- [7] So z. B. zu finden in: Kröpfl, Maximilian. Praxiskommentar zu den SCC 2021. Klausel 14 Rn. 4. Jan Sramek Verlag KG, 2021. ISBN 978-3-7097-0285-7

- die Art des Empfängers,
- der Zweck der Verarbeitung,
- die Kategorien und das Format der übermittelten personenbezogenen Daten,
- den Wirtschaftszweig, in dem die Übertragung erfolgt,
- den Speicherort der übermittelten Daten,
- die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien, sowie
- alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

- Die Bewertung ist zu dokumentieren und muss auf Anfrage der Datenschutzaufsichtsbehörde zur Verfügung gestellt werden (Klausel 14 lit. d).

3 Der EuGH und das Schrems-II-Urteil[8]

In seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18[9] (nachfolgend kurz „Schrems-II-Urteil“ genannt) stellte der EuGH bei der Interpretation der Vorgaben der DS-GVO Verschiedenes fest, was im Rahmen einer Drittland-Verarbeitung zu beachten ist. Insbesondere gehört dazu, dass ein Drittland "aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleisten [muss], dass dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist" (Rn. 104 Schrems-II-Urteil). Somit wird nicht gefordert, dass das Schutzniveau im Drittland identisch zu dem der EU ist, gefordert ist aber ein gleiches Datenschutzschutzniveau.

Bei der Beurteilung, ob das Schutzniveau im Drittland dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist, müssen vom Datenexporteur auch **potenziell mögliche Zugriffe durch staatliche Behörden** wie z. B. ein Geheimdienst oder Ermittlungsbehörden beachtet werden. Die alleinige Möglichkeit von staatlichen Zugriffen aufgrund der Gesetzlage im Drittland reicht aus, damit diese staatlichen Zugriffsmöglichkeiten im Drittland vom Datenexporteur bzgl. der Bewertung des Schutzniveaus im Drittland berücksichtigt und bewertet werden müssen. Im Schrems-II-Urteil findet sich seitens des EuGH hierzu:

> Rn. 87: Die **etwaige Verarbeitung** der betreffenden Daten durch ein Drittland **für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates stellt die Anwendbarkeit der DS-GVO auf die fragliche Übermittlung nicht in Frage**.
>
> Rn. 89, Antwort auf Vorlagefrage: Eine Übermittlung personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer **fällt in den Anwendungsbereich dieser Verordnung, wenn die Daten bei ihrer Übermittlung oder im Anschluss daran von den Behörden dieses Drittlands** für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates **verarbeitet werden können**.
>
> Rn. 105, Antwort auf Vorlagefragen 2,3 und 6: **Bei der** insoweit im Zusammenhang mit einer solchen Übermittlung vorzunehmenden **Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen**, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, **sowie**, was **einen etwaigen Zugriff der Behörden dieses Drittlands** auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes, insbesondere die in Art. 45 Abs. 2 der DS-GVO genannten Elemente."

3.1 Schrems-II-Urteil und durchsetzbare Rechte/Rechtsbehelfe

Des Weiteren führt der EuGH aus, wie die gesetzliche Anforderung „durchsetzbare Rechte und wirksame Rechtsbehelfe“ zu beurteilen ist:

> Rn. 141: […] und **gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf** einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht […].

[8] Hervorhebungen in Zitaten in den jeweiligen Randnummern des EuGH-Urteils erfolgten durch die Autoren, nicht durch das Gericht selbst

[9] EuGH, Urt. v. 2020-07-16. AZ. C-311/18 ("Schrems-II"). Online, zitiert am 2023-04-08; verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

> Rn. 105, Antwort auf Vorlagefragen 2,3 und 6: Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DS-GVO sind dahin auszulegen, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, **durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen**, dass die **Rechte der Personen**, deren personenbezogene Daten auf **der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden**, ein **Schutzniveau genießen**, das dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach **gleichwertig ist**.
>
> Rn. 57: Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 77 Abs. 1, Art. 78 Abs. 1 und Art. 79 Abs. 1 der Verordnung 2016/679 **in Verbindung mit Art. 47 der Charta** dahin **auszulegen sind** […].

In Art. 47[10] Charta der Grundrechte der Europäischen Union[11] findet sich hierzu u. a.:

> **Jede Person**, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, **hat das Recht**, **nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen** bei einem Gericht **einen wirksamen Rechtsbehelf einzulegen**.
>
> Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und **zuvor durch Gesetz errichteten Gericht** in einem **fairen Verfahren, öffentlich** und innerhalb angemessener Frist **verhandelt wird**.

Bei der Beurteilung hinsichtlich der einer betroffenen Person im Drittland zur Verfügung stehenden Rechtsmittel ist also insbesondere zu beachten:

- Hat die Person die Möglichkeit, die Rechtsmittel bei einem zuvor durch Gesetz errichteten Gericht einzulegen?
- Ist das darauf basierende Verfahren öffentlich, sodass die betroffene Person selbst an dem Verfahren teilnehmen kann?
- Ist es insgesamt ein faires Verfahren, wozu insbesondere auch die Transparenz des Verfahrens bewertet werden muss?

3.2 Schrems-II-Urteil: Resultierende Anforderungen

Im Schrems-II-Urteil leitete der EuGH diverse Anforderungen unmittelbar aus der Grundrechtecharta ab, wodurch Art. 45 DS-GVO auch dieser Sichtweise entsprechend interpretiert werden muss. Zu den Anforderungen des EuGH bzgl. einer Prüfung des Schutzniveaus in einem Drittland hinsichtlich der Verarbeitung personenbezogener Daten gehören insbesondere:

1) Die Prüfung, inwieweit im jeweiligen Drittland die Rechtsstaatlichkeit gewahrt ist, der Rechtsweg gewährleistet ist und die internationalen Menschenrechtsnormen und -standards eingehalten werden (Rn. 104 Schrems-II-Urteil).
2) Eine Prüfung, welche allgemeinen und sektorspezifischen Vorschriften, wozu auch die Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht zählen, im jeweiligen Drittland gelten (Rn. 104 Schrems-II-Urteil).
3) Eine Prüfung, ob im jeweiligen Drittland eine wirksame unabhängige Überwachung des Datenschutzes gewährleistet ist und das Recht im Drittland Mechanismen für eine

[10] Charta der Grundrechte der Europäischen Union: Artikel 47 „Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht“. Online, zitiert am 2023-04-07; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012P/TXT&from=DE#d1e697-393-1

[11] Bei der Interpretation von Art. 47 Grundrechtecharta muss insbesondere auch Art. 52 Grundrechtecharta beachtet werden. Online, zitiert am 2023-04-10; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012P/TXT&from=DE#d1e774-393-1

Zusammenarbeit mit den Datenschutzbehörden der EU-Mitgliedstaaten vorsehen (Rn. 104 Schrems-II-Urteil).

4) Eine Prüfung, ob betroffenen Personen im jeweiligen Drittland wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden (Rn. 104 Schrems-II-Urteil).
5) Eine Prüfung, ob im jeweiligen Drittland behördliche Zugriffsrechte auf personenbezogene Daten bestehen (Rn. 105 Schrems-II-Urteil).

3.3 EDSA und Schrems-II-Urteil: Empfehlungen

Basierend auf das Schrems-II-Urteil veröffentliche der Europäische Datenschutzausschuss (EDSA) im Juni 2021 „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“[12]. Darin finden sich sechs grundlegende Empfehlungen zum Vorgehen bei geplanten Verarbeitungen personenbezogener Daten in einem Drittland:

Schritt 1: Die Datenübermittlungen kennen

Alle Verarbeitungen personenbezogener Daten wie beispielsweise Übermittlungen in ein Drittland sollen im Verzeichnis der Verarbeitungen dokumentiert sein; nach Art. 30 DS-GVO existiert i. d. R. ein entsprechendes Verzeichnis für alle Verarbeitungen.

Als Verarbeitung/Übermittlung versteht der EDSA dabei jegliche Zugriffsmöglichkeit aus einem Drittland. Dies beinhaltet beispielsweise auch Zugriffe zu Wartungszwecken oder auch (Weiter-)Übermittlungen an Unterauftragnehmern in Drittländern.

Schritt 2: Auswahl der eingesetzten Übermittlungsinstrumente

Entsprechend der geplanten Drittlandverarbeitung soll der Datenexporteur das Übermittlungsinstrument nach Kapitel V der DS-GVO festlegen. In Frage kommen i. d. R.:

- Art. 45, d. h. Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der EU-Kommission,
- verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) gemäß Art. 47 DS-GVO,
- von der Kommission erlassene Standarddatenschutzklauseln (von der EU-Kommission Standardvertragsklauseln, SCC, genannt) sowie
- in einzelnen/besonderen Fällen die in Art. 49 DS-GVO enthaltenen Ausnahmeregelungen.

Schritt 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Artikel 46 DS-GVO im Hinblick auf die Gesamtumstände der Übermittlung

Sodann muss der Datenexporteur, ggf. mit Unterstützung des Datenimporteurs, die Rechtslage im Drittland beurteilt und die Effektivität der im Drittland vorgesehen Garantien bzgl. eines der EU entsprechendes gleichwertiges Schutzniveaus überprüft werden. Hierbei sind insbesondere auch die Zugriffsrechte staatlicher Stellen zu berücksichtigen.

[12] EDSA: Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten. Online, zitiert am 2023-04-07; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de

Schritt 4: Zusätzliche Maßnahmen ergreifen

Kommt der Datenexporteur zu dem Ergebnis, dass das Schutzniveau in dem Drittland nicht gleichwertig zu dem Schutzniveau der EU ist, muss er zusätzliche Maßnahmen ergreifen, welche ein entsprechendes Schutzniveau gewährleisten - oder die Verarbeitung im Drittland darf nicht erfolgen.

Als Beispiele für zusätzliche technische Maßnahmen nennt der EDSA im Anhang seiner Empfehlung die Datenverschlüsselung oder Pseudonymisierung vor Übermittlung in das Drittland, sodass im Drittland kein Zugriff auf die personenbezogenen Daten möglich ist.

Schritt 5: Verfahrensschritte nach Ermittlung effektiver zusätzlicher Maßnahmen

In diesem Schritt muss der Datenexporteur alle förmlichen Verfahrensschritte einleiten, die für die zusätzlichen Maßnahmen erforderlich sind. Z. B. muss der Datenexporteur Vorkehrungen treffen, die sicherstellen, dass Datenübertragungen umgehend ausgesetzt oder beendet werden, wenn der Datenimporteuer die ihm auferlegten Pflichten verletzt oder die zusätzlich eingerichteten Maßnahmen in dem Drittland nicht mehr sicher sind.

Schritt 6: Neubewertung in angemessenen Abständen

Der Datenexporteur ist verpflichtet, das Datenschutzniveau in dem Drittland, in das er personenbezogene Daten übermittelt, sowie die von ihm getroffenen Maßnahmen hinsichtlich der Gewährleistung des Schutzniveaus regelmäßig zu überprüfen.

Grundlegende Anforderung von EDSA besteht also darin, dass man Verarbeitungen in einem Drittland (oder Verarbeitungen durch internationale Organisationen) kennen muss. Da Verantwortliche betroffene Personen allein schon über die Absicht, Verarbeitungen in einem Drittland durchführen zu wollen, gemäß Art. 13 Abs. 1 lit. f DS-GVO bzw. Art 14 Abs. 1 lit. f DS-GVO informieren müssen, beinhaltet die Unkenntnis entsprechender Drittlandverarbeitungen regelhaft einen Verstoß gegen die Informationspflichten von Artt. 13, 14 DS-GVO.

Der Verantwortliche muss diese Verarbeitungen auch dann kennen, wenn diese Drittland-Verarbeitungen durch einen Auftragsverarbeiter initialisiert werden. Gemäß Art. 28 Abs. 2 DS-GVO benötigt ein Auftragsverarbeiter immer die Zustimmung des Verantwortlichen, wobei ein Verantwortlicher seine Zustimmung auch durch Unterlassen eines Einspruchs geben kann. Somit ist ein Verantwortlicher – wie die Bezeichnung nahelegt – immer für die Verarbeitung personenbezogener Daten in einem Drittland verantwortlich. Allerdings haftet ein Auftragsverarbeiter, wenn er entgegen den einem Verantwortlichen gegebenen vertraglichen Zusicherungen personenbezogene Daten in einem Drittland verarbeitet und hierbei nicht den Vorgaben von Kapitel V DS-GVO genügt wird.

Im Schrems-II-Urteil findet sich (Rn. 142): „Demzufolge sind der in der Union ansässige Verantwortliche und der Empfänger der Übermittlung personenbezogener Daten verpflichtet, vorab zu prüfen, ob im betreffenden Drittland das unionsrechtlich geforderte Schutzniveau eingehalten wird“. Verantwortliche müssen somit prüfen, ob einem Auftragsverarbeiter genehmigt werden kann, Verarbeitungen in einem Drittland oder auch durch in einem Drittland arbeitende Beschäftigte durchführen zu lassen, unabhängig davon, ob es sich hierbei um Unterauftragnehmer des Auftragsverarbeiters handelt oder beim Auftragsverarbeiter Beschäftigte.

Es muss daher, außer bei Nutzung eines Angemessenheitsbeschlusses nach Art. 45 DS-GVO der EU-Kommission, bei allen Verarbeitungen geprüft werden, ob die Vorgaben der DS-GVO eingehalten werden, insbesondere natürlich, ob das Schutzniveau im Drittland dem aus dem EU-Recht resultierendem Schutzniveau entspricht und ob die betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe entsprechend Art. 47 EU-Grundrechtecharta wahrnehmen können. Daher ist

die von EDSA geforderte Kenntnis, auf welchem der in Kap. V DS-GVO genannten Instrumente die Verarbeitung erfolgt, elementar: Nur bei einem Angemessenheitsbeschluss kann auf eine TIA verzichtet werden, weil diese durch die EU-Kommission erfolgte. Eine Beurteilung der Situation inkl. der Bewertung der rechtlichen Situation im Drittland ist daher ohne Angemessenheitsbeschluss der EU-Kommission unumgänglich, eine TIA somit zwingend erforderlich. Entsprechend fordert auch Klausel 14 der von der EU-Kommission veröffentlichten Standardvertragsklauseln[13] eine TIA.

[13] EU-Kommission: Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Online, zitiert am 2023-04-07; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX%3A32021D0914

4 Data Transfer Impact Assessment (TIA): Aber wie?

Es existieren keine gesetzlichen Anforderungen, wie eine TIA durchzuführen und zu dokumentieren ist. Auch seitens der Datenschutzaufsichtsbehörden finden sich zwar allgemeine Hinweise, aber keine Vorlage zur Durchführung.[14] In der Praxis gut anwendbare Vorlagen, stellt die britische Datenschutzaufsicht auf ihrer Webseite zur Verfügung.[15]

Zunächst sind administrative Daten zu erfassen, d. h. es müssen Fragen gestellt und beantwortet werden, wie beispielsweise:

- Welcher Verantwortliche oder Auftragsverarbeiter veranlasst die Drittland-Verarbeitung, ist also der Datenexporteur?
- Wer ist der Verantwortlichen oder (Unter-)Auftragsverarbeiter im Drittland (Datenimporteur)?
- In welchem Drittland erfolgt die Verarbeitung?

Anschließend ist die geplante Verarbeitung zu beschreiben. Vergleichbar den Angaben im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) muss u. a. beschrieben werden:

- Kontext und Zweck der Verarbeitung in einem Drittland,
- Betroffene Personengruppen,
- Kategorien der übermittelten personenbezogenen Daten,
- Rechtsgrundlage der Verarbeitung an sich.

Entsprechend dem Schrems-II-Urteil muss die Rechtslage im Drittland beurteilt werden, d. h. ob das im Drittland vorhandene Datenschutzniveau dem in der EU vorhandenen Schutzniveau gleichwertig ist und ob betroffene Personen durchsetzbare Rechte und wirksame Rechtsbehelfe besitzen, welchen den Vorgaben der DS-GVO wie auch der EU-Grundrechtecharta genügen. Zu den Fragen, die zu beantworten sind, gehören somit beispielsweise:

- Verfügt das Drittland bzw. die Region des Drittlandes über gesetzliche Regelungen, welche dem Datenschutz dienen?
- Gelten die Regelungen gleichermaßen für Bürger oder Einwohner des Drittlandes wie auch für Personen, welche keine Bürger oder Einwohner des Drittlandes sind?
- Unterliegt der Datenimporteur diesen Gesetzen?
- Schützen diese Regelungen auch die von der Drittland-Verarbeitung betroffenen Daten des Datenexporteurs?
- Gewähren diese Regelungen den von der Drittland-Verarbeitung betroffenen Personen durchsetzbaren Rechte und wirksamen Rechtsbehelfe, sodass im Drittland ein Schutzniveau vorhanden, welches dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist?
- Existieren im Drittland Gesetze oder Praktiken, welche den Datenimporteur zwingen können, Dritten wie Behörden Zugang zu den Daten gewähren zu müssen?

[14] Lediglich die nicht mehr zu den europäischen Aufsichtsbehörden gehörende ICO veröffentlichte 2018 eine Vorlage für eine DPIA, welche aber nicht alle Anforderungen aus dem Schrems-II-Urteil berücksichtigt: ICO (2018) sample DPIA template. Online, zitiert am 2023-04-09; verfügbar unter https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx

[15] Information Commissioner's Office (ICO) (2022) International data transfer agreement and guidance. Online, zitiert am 2023-04-07; verfügbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/
Information Commissioner's Office (ICO) (2022) Transfer risk assessments. Online, zitiert am 2023-04-07; verfügbar unter unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/

Art. 44 DS-GVO verlangt, dass alle Vorgaben der DS-GVO eingehalten werden, somit insbesondere auch die in Art. 32 DS-GVO geforderte risikobasierte Betrachtung hinsichtlich der Schutzmaßnahmen. Somit muss auch das Risiko, welches für die betroffene Person aus einer Drittlandverarbeitung erwachsen könnte, betrachtet werden. Hier ist natürlich auch zu betrachten, ob die in Kap. III DS-GVO enthaltenen Rechte der betroffenen Personen gewahrt werden, insbesondere, ob betroffene Personen über die Absicht der Drittlandverarbeitung informiert sind. Weiterhin ist das Schutzniveau der Daten zu bewerten. Hierzu gehören insbesondere Informationen:

- Sind Daten von Kindern von der Verarbeitung im Drittland betroffen?
- Sind Daten von schutzbedürftigen Erwachsenen wie z.B. Erwachsenen unter Betreuungsvorgaben oder psychisch erkrankten Personen von der Verarbeitung im Drittland betroffen?
- Sind in Art. 9 Abs. 1 DS-GVO genannte Daten von der Verarbeitung betroffen?
- Sind besonders geschützte Daten wie beispielsweise § 203 StGB unterliegende Daten von der Verarbeitung betroffen?
- Erhöht sich durch die Verarbeitung im Drittland das Risiko einer Verletzung der Rechte der Betroffenen im Drittland?
- Werden Risiken durch entsprechende technisch-organisatorische Maßnahmen eliminiert oder soweit reduziert, dass die Restrisiken aus Sicht der betroffenen Person akzeptabel sind, d. h. die Rechte der betroffenen Personen und den Schutz der personenbezogenen Daten nicht einschränken?

Entsprechend dem Schrems-II-Urteil muss auch die Möglichkeit von staatlichen Zugriffen bei einer Verarbeitung in einem Drittland oder durch internationale Organisationen betrachtet werden. Entsprechend dem Urteil des EuGH reicht die Möglichkeit eines staatlichen Zugriffs aus. Diverse Autoren befürworten, dass bei einem geringen Risiko eines staatlichen Zugriffs dieses Risiko kein Hindernis für eine Drittlandverarbeitung darstellen sollte.[16] Letztendlich muss jeder Verantwortliche für seine Verarbeitung selbst entscheiden (und dies auch bei seinen Genehmigungen von Drittlandverarbeitungen durch Auftragsverarbeiter berücksichtigen), wie er mit den Vorgaben des EuGH umgeht.[17]

Letztlich gehört zu einer abschließenden Bewertung insbesondere:

1. Die Bewertung, ob durchsetzbaren Rechte und wirksamen Rechtsbehelfe i.S.v. Art. 47 der Charta der Grundrechte der EU im Drittland existieren.
2. Die Beurteilung, ob bei der Verarbeitung im Drittland alle Vorgaben der DS-GVO eingehalten werden und insbesondere die Rechte betroffener Personen gewährleistet sind.
3. Die Darstellung und Bewertung des Risikos für die betroffenen Personen.
4. Die Wahrscheinlichkeit staatlicher Zugriffe (wenn man nicht schon die alleinige Möglichkeit als Ausschlusskriterium nimmt).
5. Die Freigabe durch eine zeichnungsberechtigte Person des Datenexporteurs.

[16] Eine dem risikobasierten Ansatz zustimmende Diskussion findet sich bspw. in: Eisenmenger F. (2023) Durchführung von Transfer Impact Assessments am Beispiel der VR China. ZD: 204-209

[17] Nach ErwGr. 20 und Fußnote 12 der aktuellen Standarddatenschutzklauseln der EU-Kommission scheint ein risikobasierter Ansatz („subjektiver Ansatz“) möglich. EDSA fordert hingegen, dass das tatsächliche vorhandene Recht bewertet werden muss (objektiver Ansatz“), z. B. in den EDSA- Empfehlungen 01/2020. Da die EU-Kommission ausdrücklich auf die Empfehlungen des EDSA verweist und eine einheitliche Auslegung der DS-GVO in Europa zu den in der DS-GVO verankerten Aufgaben des EDSA gehören, sollte im Rahmen einer Risikominimierung den Empfehlungen des EDSA gefolgt werden. Eine abschließende Rechtsprechung zu dem Thema existiert bisher nicht (wenn man vom Schrems-II-Urteil und der darin geforderten Einhaltung der Vorgaben der EU Grundrechtecharta absieht), sodass Verantwortliche für sich selbst entscheiden müssen, wie viel Risiko sie tragen wollen.

5 Excel-Tool zur Durchführung einer TIA

Es wurde eine Excel-Tabelle als Vorlage für eine TIA entworfen sowie in einer separaten Tabelle beispielhaft eine TIA für die fiktive Verarbeitung von Patientendaten durch einen amerikanischen Dienstleister durchgeführt. Beide Tabellen sind unter einer Creative Commons Lizenz[18] frei verfügbar. Obwohl die Tabellen nach bestem Wissen und Gewissen erstellt wurden, kann für die Richtigkeit der Tabellen nicht garantiert, eine Haftung nicht übernommen werden. Wer trotzdem die Tabellen nutzen möchte, findet diese unter https://gesundheitsdatenschutz.org/html/tia.php. Über Hinweise und Verbesserungsvorschläge bzgl. Aufbau, Struktur und Nutzbarkeit der Excel-Tabelle ist der Autor dankbar.

Die Excel-Tabelle besteht aus mehreren Tabellenblättern:

- **Tabellenblatt „Einführung“**
  Dieses Tabellenblatt enthält eine kurze Einführung in die TIA-Thematik, ähnlich diesem Text
- **Tabellenblatt „Adm. Angaben“**
  In diesem Tabellenblatt werden die administrativen Daten zur geplanten Verarbeitung in einem Drittland eingetragen, z. B.:
  - Wer führt Daten aus welchem Land zu wem in welches Land aus?
  - Wer erstellte wann die TIA?
  - Usw.
- **Tabellenblatt „Geplante Verarbeitung“**
  Hier erfolgt eine kurze Beschreibung,
  - um welche Verarbeitung es sich handelt,
  - welche Personengruppen von der Verarbeitung betroffen sind,
  - welche Datenkategorien verarbeitet werden sollen,
  - usw.
- **Tabellenblatt „Relevante Gesetze im Drittland“**
  Hier werden die im Drittland für die Verarbeitung relevanten Gesetze kurz dargestellt. Entsprechend den Vorgaben des EuGH folgend gehört dazu auch, welche Gesetze staatlichen Akteuren ggf. Zugriff auf die personenbezogenen Daten gewähren könnten.
- **Tabellenblatt „Bew.Drittland-Ges.“**
  Hier erfolgt eine Bewertung, ob die Gesetze im Drittland die von der geplanten Drittland-verarbeitung betroffenen Daten bzw. die Rechte der von der Drittlandverarbeitung betroffenen Personen in gleicher Weise schützen, wie es bei einer Verarbeitung in der EU bzw. EWR der Fall wäre.
- **Tabellenblatt „Risiko,betr.-Person“**
  In diesem Tabellenblatt wird betrachtet, welches Risiko die geplante Verarbeitung im betrachteten Drittland grundsätzlich für eine betroffene Person darstellt.
- **Tabellenblatt „Risiko,Behörd.-Zugriff“**
  Basierend auf vorhandenen Erfahrungswerten des Datenimporteurs wird geschätzt, wie hoch die Wahrscheinlichkeit dafür ist, dass ein staatlicher Akteur Zugriff auf die personenbezogenen Daten bekommt.
- **Tabellenblatt „Risiko,Massenüberwachung“**
  Wird eine Transportverschlüsselung, die dem Stand der Technik entspricht, genutzt, wird dieses Tabellenblatt ausgeblendet, da die personenbezogenen Daten im Rahmen einer

[18] Creative Commons (CC): Lizenz „Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)“. Online, zitiert am 2023-04-07; verfügbar unter https://creativecommons.org/licenses/by-sa/4.0/deed.de

Massenüberwachung nicht unverschlüsselt abgefangen werden können, somit keine Gefahr einer unbefugten Kenntnisnahme der Daten besteht.
Sollte jedoch keine Transportverschlüsselung eingesetzt werden, so muss dieses Risiko betrachtet und bewertet werden.
Ein- bzw. Ausblenden erfolgt über die Antwort auf die Frage „Wie erfolgt die Übertragung der Daten?“ in Zeile 10 im Tabellenblatt „Risiko,betr.-Person“.

- **Tabellenblatt „Begriffsbestimmungen“**
  Dieses Tabellenblatt wurde eingefügt, damit in den verschiedenen Tabellenblättern verwendete Begriffe wie beispielsweise „Datenexporteur“ nachgelesen werden können.
- **Tabellenblatt „Links“**
  In diesem Tabellenblatt sind ausgewählte Internetadressen zu finden, die für eine TIA relevant sein können. Hier sind z. B. Internetadressen für die aktuellen SCC zu finden oder auch ein Link zum Schrems-II-Urteil.
- **Tabellenblatt „Literatur“**
  Wie der Name es schon andeutet, finden sich hier Literaturhinweise zum Thema Verarbeitung in Drittländern.
- **Tabellenblatt „Hilfstexte“**
  Dieses Tabellenblatt ist standardmäßig ausgeblendet. Es enthält Ausfülltexte, die in einigen Tabellenblättern genutzt werden.

Die Tabellenblätter enthalten Fragen, die häufig mit vorausgefüllten Werten beantwortet werden. Viele Fragen enthalten „Ja/Nein“-Möglichkeiten, aber es gibt auch umfangreichere Antwortmöglichkeiten (siehe Abbildung 1).

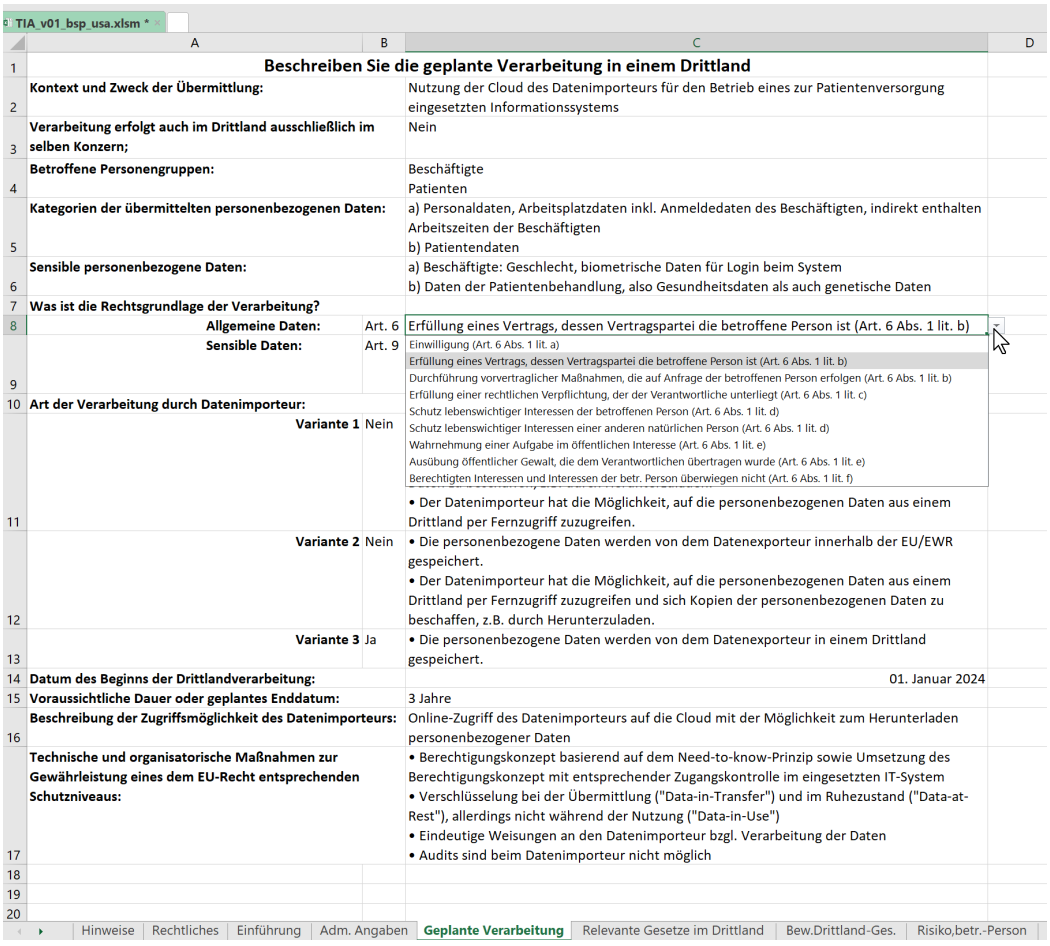
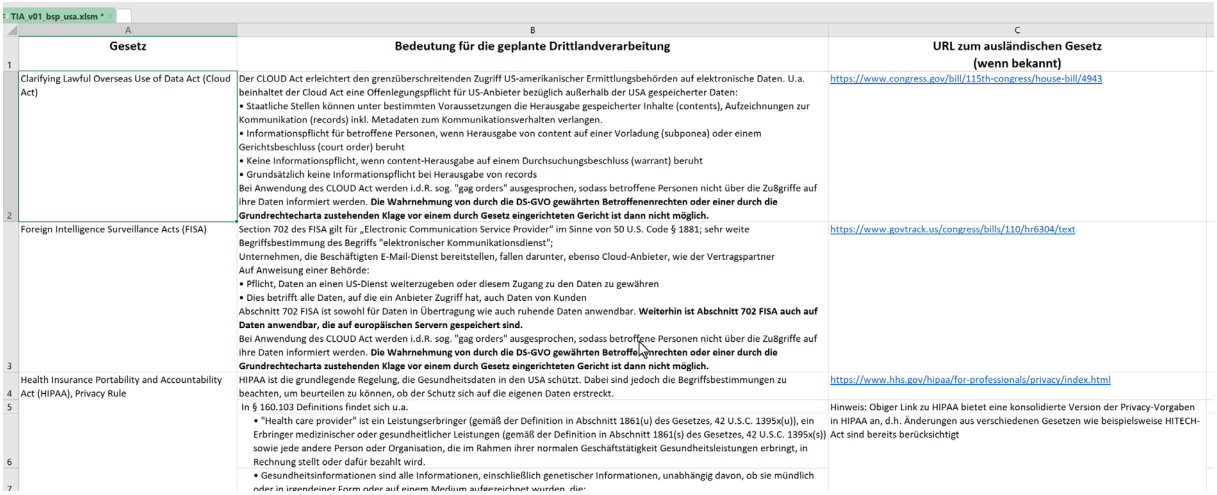


Abbildung 1: Beispiel für Antwortmöglichkeiten

In anderen Bereichen, wie beispielsweise der Darstellung der im Drittland geltenden und für die Verarbeitung relevanten Gesetze, muss Freitext eingetragen werden (siehe Abbildung 2).



TIA_v01_bsp_usa.xlsm *

	A	B	C
1	**Gesetz**	**Bedeutung für die geplante Drittlandverarbeitung**	**URL zum ausländischen Gesetz (wenn bekannt)**
2	Clarifying Lawful Overseas Use of Data Act (Cloud Act)	Der CLOUD Act erleichtert den grenzüberschreitenden Zugriff US-amerikanischer Ermittlungsbehörden auf elektronische Daten. U.a. beinhaltet der Cloud Act eine Offenlegungspflicht für US-Anbieter bezüglich außerhalb der USA gespeicherter Daten: • Staatliche Stellen können unter bestimmten Voraussetzungen die Herausgabe gespeicherter Inhalte (contents), Aufzeichnungen zur Kommunikation (records) inkl. Metadaten zum Kommunikationsverhalten verlangen. • Informationspflicht für betroffene Personen, wenn Herausgabe von content auf einer Vorladung (subponea) oder einem Gerichtsbeschluss (court order) beruht • Keine Informationspflicht, wenn content-Herausgabe auf einem Durchsuchungsbeschluss (warrant) beruht • Grundsätzlich keine Informationspflicht bei Herausgabe von records Bei Anwendung des CLOUD Act werden i.d.R. sog. "gag orders" ausgesprochen, sodass betroffene Personen nicht über die Zugriffe auf ihre Daten informiert werden. **Die Wahrnehmung von durch die DS-GVO gewährten Betroffenenrechten oder einer durch die Grundrechtecharta zustehenden Klage vor einem durch Gesetz eingerichteten Gericht ist dann nicht möglich.**	https://www.congress.gov/bill/115th-congress/house-bill/4943
3	Foreign Intelligence Surveillance Acts (FISA)	Section 702 des FISA gilt für „Electronic Communication Service Provider" im Sinne von 50 U.S. Code § 1881; sehr weite Begriffsbestimmung des Begriffs "elektronischer Kommunikationsdienst"; Unternehmen, die Beschäftigten E-Mail-Dienst bereitstellen, fallen darunter, ebenso Cloud-Anbieter, wie der Vertragspartner Auf Anweisung einer Behörde: • Pflicht, Daten an einen US-Dienst weiterzugeben oder diesem Zugang zu den Daten zu gewähren • Dies betrifft alle Daten, auf die ein Anbieter Zugriff hat, auch Daten von Kunden Abschnitt 702 FISA ist sowohl für Daten in Übertragung wie auch ruhende Daten anwendbar. **Weiterhin ist Abschnitt 702 FISA auch auf Daten anwendbar, die auf europäischen Servern gespeichert sind.** Bei Anwendung des CLOUD Act werden i.d.R. sog. "gag orders" ausgesprochen, sodass betroffene Personen nicht über die Zugriffe auf ihre Daten informiert werden. **Die Wahrnehmung von durch die DS-GVO gewährten Betroffenenrechten oder einer durch die Grundrechtecharta zustehenden Klage vor einem durch Gesetz eingerichteten Gericht ist dann nicht möglich.**	https://www.govtrack.us/congress/bills/110/hr6304/text
4	Health Insurance Portability and Accountability Act (HIPAA), Privacy Rule	HIPAA ist die grundlegende Regelung, die Gesundheitsdaten in den USA schützt. Dabei sind jedoch die Begriffsbestimmungen zu beachten, um beurteilen zu können, ob der Schutz sich auf die eigenen Daten erstreckt.	https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
5		In § 160.103 Definitions findet sich u.a.	Hinweis: Obiger Link zu HIPAA bietet eine konsolidierte Version der Privacy-Vorgaben in HIPAA an, d.h. Änderungen aus verschiedenen Gesetzen wie beispielsweise HITECH-Act sind bereits berücksichtigt
6		• "Health care provider" ist ein Leistungserbringer (gemäß der Definition in Abschnitt 1861(u) des Gesetzes, 42 U.S.C. 1395x(u)), ein Erbringer medizinischer oder gesundheitlicher Leistungen (gemäß der Definition in Abschnitt 1861(s) des Gesetzes, 42 U.S.C. 1395x(s)) sowie jede andere Person oder Organisation, die im Rahmen ihrer normalen Geschäftstätigkeit Gesundheitsleistungen erbringt, in Rechnung stellt oder dafür bezahlt wird.	
7		• Gesundheitsinformationen sind alle Informationen, einschließlich genetischer Informationen, unabhängig davon, ob sie mündlich oder in irgendeiner Form oder auf einem Medium aufgezeichnet wurden, die:	

Abbildung 2: Beispiel für Freitext-Eingabe

Im Tabellenblatt „Bewertung" werden Aussagen ausgewertet und Hinweise gegeben (siehe Abbildung 3). Der Hinweis „Verboten" bedeutet nicht, dass grundsätzlich eine Verarbeitung im Drittland nicht möglich wäre. „Verboten" muss i. S. v. „Verarbeitung ist im Drittland nicht möglich, wenn der Zugriff auf die personenbezogenen Daten nicht wirksam verhindert wird". Dies kann beispielsweise durch eine dem Stand der Technik entsprechende Verschlüsselung erfolgen, wobei die Schlüssel dann ausschließlich in der Verfügungsgewalt des Datenexporteurs liegen müssen. Kann kein Dritter, auch keine staatliche Behörde des Drittlandes, Zugriff auf die personenbezogenen Daten erhalten, ist eine Verarbeitung trotz gegenstehender gesetzlicher Rahmenbedingungen möglich. So kann beispielsweise ein entsprechend verschlüsseltes Backup in einer Cloud in einem entsprechenden Drittland gespeichert werden, wenn das Backup erst bei der Wiederherstellung in Europa entschlüsselt wird und so im Drittland keine Person und/oder Behörde Zugriff auf die Daten erhalten kann.

Daher obliegt die Entscheidung, ob eine Verarbeitung in einem Drittland durchgeführt werden soll oder nicht, ausschließlich beim Datenexporteur, also bei einer natürlichen oder juristischen Person (siehe Abbildung 3).

	Existieren durchsetzbaren Rechte und wirksamen Rechtsbehelfe i.S.v. Art. 47 der Charta der Grundrechte der EU?	Nein	
	Werden die in Kap. III DS-GVO beschriebenen Rechte von betroffenen Personen gewährleistet?	Ja	
	Insbesondere: Wird die jeweils betroffene Person über den behördlichen Zugriff informiert, sodass sie Rechtsbehelfe wahrnehmen kann?	Nein	Die Verarbeitung muss unterbleiben
	Risiko für die betroffenen Personen:	**Hoch**	
	Wahrscheinlichkeit, dass personenbezogene Daten im Rahmen einer Massenüberwachung unbefugt offenbart werden:	9,75%	
	Ausgehend von den oben gegebenen Antworten ist die Verarbeitung in einem Drittland:	**Verboten**	Verboten i.S.v. "Verarbeitung im Drittland nicht möglich", wenn der Zugriff auf die personenbezogenen Daten nicht wirksam verhindert wird, wie beispielsweise durch eine dem Stand der Technik entsprechende Verschlüsselung, wobei die Schlüssel dann ausschließlich in der Verfügungsgewalt des Datenexporteurs liegen müssen.
		Zu beachten:	Für die betroffenen Personen liegt bei der Verarbeitung ein hohes Risiko vor. Daher müssen entsprechend hohe Schutzmaßnahmen die Sicherheit der Verarbeitung gewährleisten. Dies betrifft insbesondere Schutzmaßnahmen, die eine aus Sicht des EU-Rechts unbefugte Kenntnisnahme sicher verhindert.
	Bewertung der getroffenen/vereinbarten technischen Maßnahmen:	Technische Maßnahmen sehen gut aus	
	Bewertung der getroffenen/vereinbarten organisatorischen Maßnahmen:	Organisatorische Maßnahmen sehen gut aus	
	Entscheidung des Datenimporteurs (Zeichnungsberechtigte Person): Freigabe zur Drittlandverarbeitung wird	**Erteilt**	**Begründung:** 1) Die eingesetzte Verschlüsselung stellt zuversichtlich sicher, dass Behörden im Drittland keine Daten einsehen können 2) Der Datenimporteur sicherte vertraglich zu, dass er vollumfänglich Daten Dritten, inkl. Behörden, überlässt, wenn dies nach dem Recht, welchem der Datenexporteur unterliegt, nicht zulässig ist.
		Freigebender:	Frau Luise Gottesstrafe, Geschäftsführerin

Abbildung 3: Hinweise im Tabellenblatt "Bewertung"

6 Abkürzungen

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Art.	Artikel
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DTIA	Data Transfer Impact Assessment
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
ErwGr.	Erwägungsgrund / Erwägungsgründe
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
i. d. R.	in der Regel
i. S.	im Sinne
i. S. d.	im Sinne der / des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
Kap.	Kapitel
lit.	littera (lat. „Buchstabe“)
Rn.	Randnummer
SCC	Standarddatenschutzklauseln, von der EU-Kommission Standardvertragsklauseln genannt (engl. „standard contractual clauses“)
TIA	Transfer Impact Assessment
Urt.	Urteil
vgl.	vergleiche
VO	Verordnung

7 Literaturhinweise

7.1 Zeitschriftenbeiträge

- Baumgartner U, Hansch G, Roth H. (2021) Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten. ZD: 608-614
- Bergt M. (2022) Datenschutzrechtliche Anforderungen an den Einsatz von US-Cloud-Anbietern - nicht nur in Vergabeverfahren. CR: 629-635
- Dehmel S, Ossmann-Magiera L. (2023) Drittstaatentransfers nach Schrems II. Wie können Daten international übermittelt werden und gleichzeitig ein angemessenes Datenschutzniveau gewährleisten? MMR: 17-22
- Determann L, Lutz H, Nebel M. (2022) International Data Transfer and Trade Restraints. Cri: 140-146
- Determann L, Lutz H, Nebel M. (2022) Internationale Datenübermittlungen. IWRZ: 204-208
- Diercks N, Roth HM. (2021) Datenübermittlung in unsichere Drittstaaten. ZdiW: 313 - 320
- Drechsler L. (2022) Defining personal data transfers for the context of the General Data Protection Regulation. A critical perspective on the Guidelines 5/2021 of the European Data Protection Board. PinG: 24-29
- Eichmann N, Nowak JN. (2021) Zum Rechtsrahmen für den transatlantischen Datenverkehr. RDV: 194-199
- Eisenmenger F. (2023) Durchführung von Transfer Impact Assessments am Beispiel der VR China. ZD: 204-209
- Glocker F. (2023) EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmass. Entwurf des Angemessenheitsbeschlusses der EU-Kommission und seine Erfolgsaussichten vor dem EuGH. ZD: 189-194
- Kremer S. (2021) Arbeitsteilige Verarbeitungen: Wer übermittelt die Daten ans Drittland? CR: 719-730
- Lejeune M. (2021) Datenaustausch mit Drittländern auf der Grundlage der neuen EU-Standardvertragsklauseln. ITRB: 293-299
- Lejeune M. (2022) Datentransfer mit den USA auf der Grundlage der Executive Order von Präsident Biden vom 7.10.2022 Wann ist der Datenschutz in Drittstaaten wie den USA adäquat? CR: 775-785
- RoßnagelA. (2022) Internationaler Datentransfer. Stand und Perspektiven. DuD: 545-549
- Sandfuchs B. (2021) The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II. GRUR Int.: 245-249
- Schmitz B, Spies A. (2022) DSK: US-Gutachten zur Risikoeinschätzung bei Datentransfers (DTIA) veröffentlicht. ZD-Aktuell: 01051
- Voigt P. (2021) Neue Standardvertragsklauseln für internationale Datentransfers. Überblick und Praxistauglichkeit. CR: 458-465
- Zanon NB, Petersen E. (2021) Neue Perspektive für Drittlandsübermittlungen? Änderungen und Neuerungen durch die neuen Standarddatenschutzklauseln der EU-Kommission. ITRB: 189-193

7.2 Bücher

- Kröpfl, Maximilian. Praxiskommentar zu den SCC 2021. EU Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer. Jan Sramek Verlag KG, 2021. ISBN 978-3-7097-0285-7
- Seak, Sabrina. Grenzen der Datenübermittlungen aus der EU in Drittstaaten – anhand des Beispiels der USA. Verlag Duncker & Humblot GmbH, 2022. ISBN 978-3-428-18505-4
- Wittershagen, Leonie. The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit. Walter de Gruyter GmbH,2023. ISBN 978-3-11-099933-4

7.3 Internet

- bitkom (2022) Verarbeitung personenbezogener Daten in Drittländern. Version 1.3, Auf Basis der EU-Datenschutz-Grundverordnung post Schrems II. Online, zitiert am 2023-04-09; verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Verarbeitung-personenbezogener-Daten-Drittlaender
- DSK (2022-11-15) Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages. Online, zitiert am 2023-04-09; verfügbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Kurzgutachten_Facebook-Fanpages_V1_1_clean.pdf
- EDSA (2021) Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten. Version 2.0. Online, zitiert am 2023-04-09; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/ recommendations/recommendations-012020-measures-supplement-transfer_de
- ICO (2022) Data protection impact assessments. Online, zitiert am 2023-04-09; verfügbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- ICO (2018) Sample DPIA template. Online, zitiert am 2023-04-09; verfügbar unter https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx
- ICO (2022) International data transfer agreement and guidance. Transfer Impact Assessment Templates. Online, zitiert am 2023-04-09; verfügbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/
- ICO (2022) Transfer risk assessments. Online, zitiert am 2023-04-09; verfügbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/
- International Association of Privacy Professionals (IAPP, 2021) Online, zitiert am 2023-04-09; verfügbar unter https://iapp.org/resources/article/transfer-impact-assessment-templates/
- Microsoft (2023) Data Protection Impact Assessment for the GDPR. Online, zitiert am 2023-04-09; verfügbar unter https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-protection-impact-assessments
- Österreichische Datenschutzbehörde (2021) Teilbescheid D155.027, 2021-0.586.257: Einsatz von Google Analytics auf der Basis von Standarddatenschutzklauseln unzulässig. Online, zitiert am 2023-04-09; verfügbar unter https://www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf

7.4 Gutachten zur Rechtslage in Drittstaaten

- DSK (2022-01-25) Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse (Deutsch). Online, zitiert am 2023-04-09; verfügbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf
- DSK (2022-01-25) Wesentliche Befunde des Gutachtens von Stephen I. Vladeck vom 15.11.2021 zur Rechtslage in den USA. Online, zitiert am 2023-04-09; verfügbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/20220125_dsk_vladek.pdf
- EDSA (2021-11-08) Legal study on Government access to data in third countries. (China, India, Russia) Online, zitiert am 2023-04-09; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-government-access-data-third_en

Anhang: Makros in Excel prüfen

Office-Dateien mit einem „x“ in der Dateiendung wie beispielsweise docx oder xlsx sind nichts anderes als zip-Dateien. Daher kann man durch Umbenennen und Anfügen der Dateiendung „.zip“ eine Datei problemlos in einem Dateiexplorer öffnen und sich den Inhalt der entsprechenden Office-Datei ansehen. Auch Excel-Dateien mit enthaltenen Makros (xlsm-Dateien) sind nichts anderes als zip-Dateien und können so geöffnet werden. Fast alle in der zip-Datei enthaltenen Dateien sind xml-Dateien, die mit jedem beliebigen Text-Editor angesehen und verändert werden können. Ausgerechnet die VBA-Makros sind jedoch Binärdateien, sodass man den VBA-Code auf diese Weise nicht prüfen kann (siehe Abbildung 4).

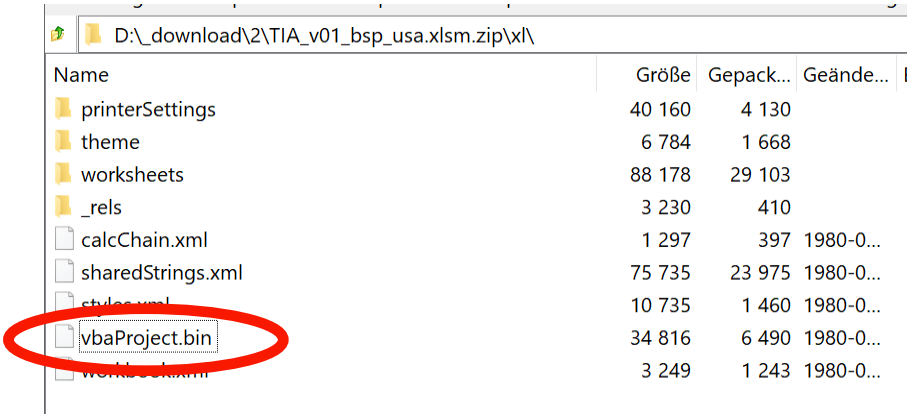


Abbildung 4: Mit "zip"-Endung versehene und geöffnete Exce--Tabelle

Öffnet man eine Excel-Datei mit einem Makro, werden Makros von Excel zunächst einmal aber nicht ausgeführt. Stattdessen erhält man eine Sicherheitswarnung (siehe Abbildung 5).

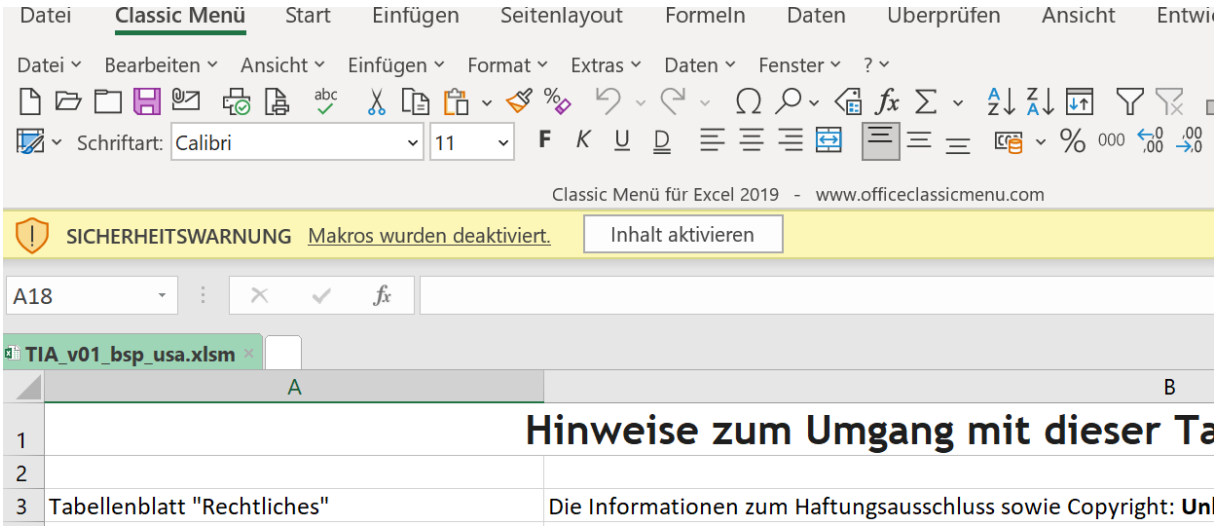


Abbildung 5: Warnung vor Makros bei Öffnen einer Excel-Tabelle mit Makros

Das oder die enthaltenen Makros werden erst aktiviert, wenn man auf „Inhalt aktivieren“ klickt.[19] Bevor man klickt, sollte man sich jedoch die enthaltenen Makros ansehen. Hierzu klickt man in der Registerkarte „Entwicklertools“[20] und dort auf „Visual Basic“ (siehe Abbildung 6).

[19] Microsoft sperrt bei aus dem Internet stammenden Excel-Dateien alle Makros. Einen Hinweis zum Entsperren findet man unter https://support.microsoft.com/de-de/topic/ein-potenziell-gef%C3%A4hrliches-makro-wurde-blockiert-0952faa0-37e7-4316-b61d-5b5ed6024216

[20] Eine Anleitung, wie man die Registerkarte in Excel zum Menu hinzufügt, findet man bei Microsoft. Online, zitiert am 2023-04-09; verfügbar unter https://support.microsoft.com/de-de/office/anzeigen-der-registerkarte-entwicklertools-e1192344-5e56-4d45-931b-e5fd9bea2d45

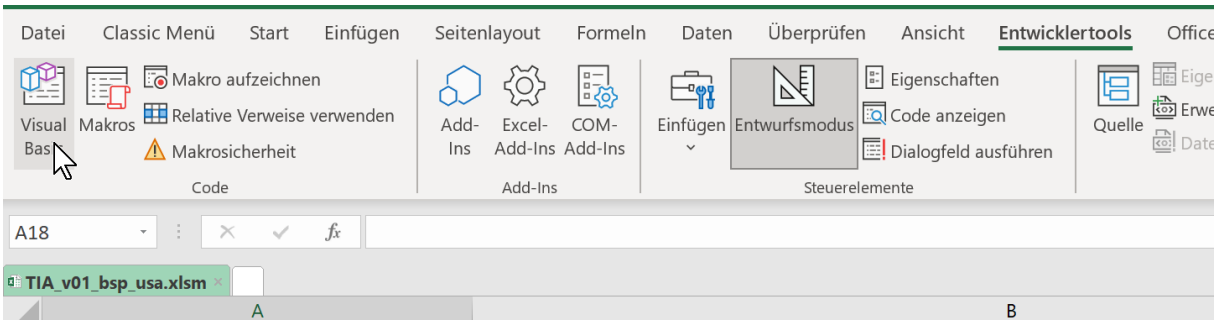


Abbildung 6: Aufruf des VBA-Editors in Excel

Daraufhin öffnet sich der Visual Basic Editor von Microsoft und die in der Tabelle enthaltenen Makros werden angezeigt (siehe Abbildung 7).

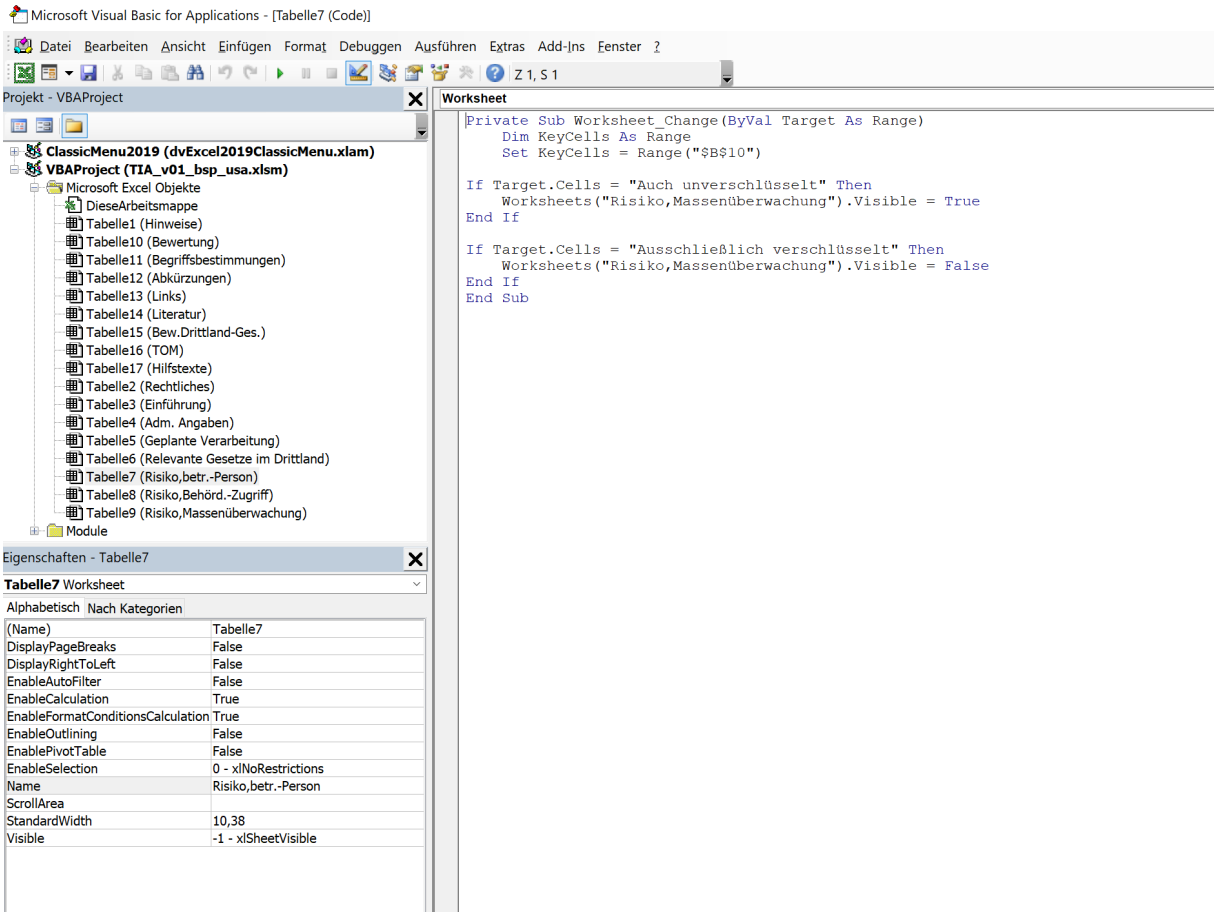


Abbildung 7: In TIA-Tabelle enthaltenes Makro zum Ein- und Ausblenden eines Tabellenblattes

In der Excel-Tabelle zur TIA befindet sich ein einziges Makro, welches ein anderes Tabellenblatt in Abhängigkeit eines bestimmten Zellwertes in einem Tabellenblatt ein- oder ausblendet. Der entsprechende VBA-Code lautet:

```
Private Sub Worksheet_Change(ByVal Target As Range)
        Dim KeyCells As Range
        Set KeyCells = Range("$B$10")
If Target.Cells = "Auch unverschlüsselt" Then
        Worksheets("Risiko,Massenüberwachung").Visible = True
        End If
If Target.Cells = "Ausschließlich verschlüsselt" Then
```

```
        Worksheets("Risiko,Massenüberwachung").Visible = False
        End If
    End Sub
```

Hat man sich die Makros angesehen und geprüft, ob diese ungefährlich sind, muss die Tabelle geschlossen und erneut geöffnet werden, damit mit einem erneuten Klick auf „Inhalt aktivieren“ (siehe Abbildung 5) das Makro aktiviert wird.