Praxishinweise zum Fragebogen „konzerninterner Datenverkehr“ der Aufsichtsbehörden hinsichtlich Schrems II

Die Hinweise sind für ein besseres Verständnis der Fragebögen gedacht. Passen Sie daher bitte die jeweilige Antwort an die Gegebenheiten Ihres Unternehmens bzw. Unternehmensverbundes an. Führen Sie Ihre Antworten möglichst kurz und prägnant aus und antworten Sie nur auf gestellte Fragen.

Einleitung

Anlässlich einer koordinierten Kontrolle von grenzüberschreitenden Datenübermittlungen in Drittländer seitens der deutschen Aufsichtsbehörden sollen ausgewählte Unternehmen auf Basis eines Fragenkataloges angeschrieben werden[1]. Insgesamt fünf Themenbereiche werden von unterschiedlichen Fragebögen[2] abgedeckt. Diese sind:

- Bewerberportale
- Konzerninterner Datenverkehr
- Mailhoster
- Tracking
- Webhoster

Hintergrund ist das Urteil des EuGH zu Schrems II. Dort wurde zum einen festgestellt, dass Übermittlungen in die USA nicht länger auf Basis des EU-U.S.-Privacy Shields[3] erfolgen können. Die Verwendung von EU-Standardvertragsklauseln steht unter dem Vorbehalt, dass der Datenimporteur im Drittland keinen Gesetzen unterliegt, die ihm die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

Die GDD möchte betroffene Unternehmen und deren Datenschutzbeauftragte unterstützen und allgemeine Hinweise zur Beantwortung des Fragebogens zum **konzerninternen Datenverkehr geben**. Teile dieser Fragen werden auch in den übrigen Fragebögen verwendet, so dass diese Hinweise dort ebenfalls Gültigkeit haben.

Frage 1: Übermittelt Ihr Unternehmen personenbezogene Daten an andere Unternehmen des Konzerns mit Sitz außerhalb des EWR? Bitte beachten Sie, dass es sich auch schon dann um eine Übermittlung im Sinne des Kapitel V DS-GVO handelt, wenn Daten, die z.B. in Deutschland gespeichert sind, von einer in einem Drittland befindlichen Person per Fernzugriff aufgerufen werden können.

Hinweise: Die Übermittlung wird in der DS-GVO nicht definiert. Sie wird in Gestalt einer „Offenlegung durch Übermittlung“ als Unterfall der Verarbeitung erwähnt (Art. 4 Nr. 2 DS-GVO). Wie es der Fragebogen bereits andeutet, wird die Übermittlung personenbezogener Daten in der Grundverordnung weit ausgelegt. Daten müssen nicht aktiv übertragen werden, um übermittelt zu werden. Es genügt auch eine Zugriffsmöglichkeit aus dem Drittland auf personenbezogene Daten, die in der EU gespeichert sind. Abzugrenzen ist die Übermittlung grundsätzlich von einer Direkterhebung personenbezogener Daten aus einem Drittland heraus. Dieser Vorgang vollzieht sich außerhalb der Regeln des Kapitel V. In einem Konzernumfeld ist die Direkterhebung aus dem Drittland jedoch die Ausnahme. Hier werden personenbezogene Daten regelmäßig durch eine europäische Niederlassung zunächst verarbeitet und im Zuge dessen in ein Drittland exportiert.

Liegen Übermittlungen in ein Drittland vor, ist die Frage der Aufsichtsbehörden entsprechend positiv zu beantworten.

[1] https://datenschutz-hamburg.de/pressemitteilungen/2021/06/2021-06-01-fragebogen-datentransfer

[2] https://datenschutz-hamburg.de/pages/fragebogenaktion/

[3] https://www.privacyshield.gov/

Bei den Empfängern sind im Weiteren lediglich Unternehmen des Konzerns im Drittland zu nennen, nicht konzernfremde Dienstleister.

Folgefrage: Um welche Daten und um welche Unternehmen in welchem Drittland handelt es sich?

Hinweise: An dieser Stelle hat eine Beschreibung der von der Übermittlung betroffenen personenbezogenen Daten zu erfolgen. Der Fragebogen spezifiziert nicht, ob Daten oder Datenkategorien anzugeben sind. Es würde sich an dieser Stelle anbieten, verfügbare Informationen aus dem Verzeichnis von Verarbeitungstätigkeiten heranzuziehen oder bspw. Beschreibungen zu Daten bzw. Datenkategorien aus Verträgen mit Datenempfängern im Drittland. Es sollten sich aus den Beschreibungen zumindest hinreichende Informationen zu den Umständen der Datenverarbeitung ergeben. Hierzu gehört zum einen die Datenkategorie (personenbezogene Kunden- oder Beschäftigtendaten, Gesundheitsdaten etc.) aber auch weitergehende Angaben zur weiteren Einordnung eines Datums (Log-Dateien, Metadaten, Gesprächsinhalte etc.).

Ferner sind die konkreten Empfänger personenbezogener Daten mit ihrer Firmierung ebenso zu nennen, wie das Land des Unternehmenssitzes.

Insgesamt ist es sinnhaft, die Darstellung thematisch anhand der einschlägigen Datenkategorie anzuordnen.

Frage 2: Übermittelt Ihr Unternehmen personenbezogene Daten an andere Unternehmen des Konzerns mit Speicherort außerhalb des EWR?

Hinweise: Frage 2 ist mit Frage 1 fast deckungsgleich, zielt jedoch auf eine Speicherung personenbezogener Daten im Drittland ab. Werden personenbezogene Daten an Konzernunternehmen im Drittland übermittelt und dort zumindest temporär gespeichert, ist diese Frage mit „ja“ zu beantworten.

Um welche Daten und um welche Unternehmen in welchem Drittland handelt es sich und in welchem Drittland befindet sich der Speicherort?

Hinweise: Auch an dieser Stelle wird keine Unterscheidung zwischen Daten oder Datenkategorien vorgenommen. Es gelten auch hier die Ausführungen zu Frage 1, wobei sich die Angabe des Drittlands auf den Speicherort personenbezogener Daten bezieht.

Frage 3: Seit wann und in welchem Intervall erfolgen die Übermittlungen nach Ziff. 1 und 2?

Hinweise: An dieser Stelle sind die tatsächlichen Übermittlungen personenbezogener Daten mit einem Startzeitpunkt anzugeben. Sollte dies nicht aus Übertragungsprotokollen bekannt sein, können Angaben aus Konzernverträgen beispielsweise Aufschluss hierüber geben. Bezüglich des Intervalls ist von besonderem Interesse, ob eine Übermittlung nur einmalig, gelegentlich oder regelmäßig erfolgt.

Hintergrund sind zum einen die Ausführungen in ErwG 111 zu den Ausnahmen von einem angemessenen Datenschutzniveau beim Drittlandstransfer (vgl. Art. 49 DS-GVO). Bestimmte Ausnahmen von einem angemessenen Datenschutzniveau stehen insbesondere nach aufsichtsbehördlicher Meinung unter dem Vorbehalt einer nur gelegentlichen Übermittlung.

Darüber hinaus dürfte es aus allgemeinen Risikogesichtspunkten bereits einen Unterschied machen, ob personenbezogene Daten regelmäßig oder nur in seltenen Fällen an einen Empfänger im Drittland übermittelt werden, so beispielsweise hinsichtlich behördlicher Zugriffsmöglichkeiten auf personenbezogene Daten.

Frage 4: Zu welchen Zwecken und aufgrund welcher datenschutzrechtlichen Grundlage erfolgen die Übermittlungen nach Ziff. 1 und 2? Ist die Rechtsgrundlage Art. 6 DS-GVO, nennen Sie bitte den konkreten Absatz und Buchstaben.

Hinweise: Übermittlungen personenbezogener Daten in ein Drittland, haben die sog. 2-Stufen-Prüfung zu durchlaufen. Auf der ersten Prüfstufe ist insbesondere die Zulässigkeit der Datenweitergabe zu prüfen. Insoweit zielt diese Frage auf die Zulässigkeit der Übermittlung im Rahmen der ersten Prüfstufe ab.

Zunächst sind die Übermittlungen jeweils anhand ihrer Zwecke zu beschreiben. Der Zweck muss hinreichend konkret beschrieben werden (z.B. Personalverwaltung, Customer Relationship Management, IT- Service und Support, Lieferantenverwaltung etc.).

Informationen zu den Zwecken sind regelmäßig dem Verarbeitungsverzeichnis zu entnehmen.

Für jeden Zweck der Übermittlung ist sodann eine dezidierte Rechtsgrundlage aus der DS-GVO oder dem BDSG anzugeben. Es ist zu erwarten, dass sich Rechtsgrundlagen an dieser Stelle wiederholen werden.

Frage 5: Auf welche rechtlichen Grundlagen bzw. Übermittlungsinstrumente im Sinne von Kapitel V DS-GVO werden die Drittlandsübermittlungen nach Ziff. 1 und 2 gestützt?

Hinweise: Kapitel V regelt die Anforderungen zur Wahrung eines angemessenen Datenschutzniveaus beim Datenempfänger im Drittland (zweite Prüfstufe im Rahmen des Drittlandstransfers).

Grundsätzlich ist für jeden Zweck einer Übermittlung eines der Instrumente aus Kapitel V zu identifizieren. Der Fragebogen fordert eine solche Aufschlüsselung jedoch an dieser Stelle nicht. Es genügt eine pauschale Angabe der für alle Drittlandstransfers eingesetzten Werkzeuge bzw. Ausnahmen von einem angemessenen Datenschutzniveau. Unter dem Punkt „Anderes/Erläuterung“ können insbesondere eigene Verträge mit Dienstleistern (sog. Ad-hoc-Verträge) genannt werden. Solche Verträge werden in der Praxis jedoch sehr selten benutzt, zumal sie seitens der zuständigen Aufsichtsbehörde genehmigt werden müssen.

Frage 6: Wenn Sie die Datenübermittlungen in die USA oder andere Drittländer auf Standarddatenschutzklauseln (SDK) gemäß Art. 46 Abs. 2 lit. c oder Art. 46 Abs. 5 Satz 2 DS-GVO stützen, teilen Sie uns bitte mit, mit wem Sie solche SDK unterzeichnet haben, geben Sie an, welche Vorlage der Kommission für den Abschluss von SDK verwendet wurde (SDK für die Übermittlung von personenbezogenen Daten zwischen zwei für die Verarbeitung Verantwortlichen oder SDK für die Übermittlung von personenbezogenen Daten an in Drittländern ansässige Auftragsverarbeiter) und übermitteln Sie eine unterzeichnete Kopie.

Hinweise: Standarddatenschutzklauseln der Kommission (oftmals referenziert als EU-Standardvertragsklauseln oder SCC) könnten als Garantie für die Übermittlung personenbezogener Daten in ein Drittland grundsätzlich verwendet werden. Sie wurden erst kürzlich in einer neuen Fassung verabschiedet[4]. Die Klauseln berücksichtigen grundsätzlich folgende Übermittlungskonstellationen:

- Übermittlung personenbezogener Daten von einem Verantwortlichen in der EU an einen Verantwortlichen im Drittland (Controller-to-Controller, C2C)
- Übermittlung personenbezogener Daten von einem Verantwortlichen in der EU an einen Auftragsverarbeiter im Drittland (Controller-to-Controller, C2P)
- Übermittlung personenbezogener Daten von einem Auftragsverarbeiter in der EU an einen Auftragsverarbeiter im Drittland (Processor-to-Processor, P2P)
- Übermittlung personenbezogener Daten von einem Auftragsverarbeiter in der EU an einen Verantwortlichen im Drittland (Processor-to-Controller, P2C)

An dieser Stelle des Fragebogens ist die Art der verwendeten Standarddatenschutzklauseln anzugeben. Werden zum Beispiel die Varianten „C2C“ und „C2P“ eingesetzt, sind beide Varianten im Fragebogen anzukreuzen. Die Konstellation„P2C“ findet im Fragebogen noch keine Erwähnung, da dieser vor Verabschiedung der neuen Standarddatenschutzklauseln veröffentlicht wurde.

Im Weiteren sind die konkreten Vertragspartner anzugeben, mit denen die Standarddatenschutzklauseln vereinbart wurden.

Frage 7: Wenn Sie solche SDK abgeschlossen haben, haben Sie dann (mit den Empfängern) eine sorgfältige Bewertung der Rechtsordnung des Drittlandes vorgenommen?

Hinweise: Der EuGH hat in seinem Urteil zu Schrems II daran erinnert, dass die Verarbeitung der

[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-dataprotection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_de

personenbezogenen Daten im Einklang der DS-GVO zu erfolgen hat. Dies gilt insbesondere mit Blick auf entgegenstehende Rechte, die für den Datenimporteur im Drittland gelten und den dortigen Behörden Zugriffsmöglichkeiten auf personenbezogene Daten geben. Hierbei sind die maßgeblichen Elemente der Rechtsordnung des jeweiligen Landes zu berücksichtigen.

Datenexporteure haben sich grundsätzlich mit der für den Importeur geltenden Rechtsordnung auseinander zu setzen. Dies sollte die Kriterien aus den Angemessenheitsbeschlüssen der Kommission gem. Art 45 Abs. 2 DS-GVO berücksichtigen.

Weitere Anforderungen an eine „sorgfältige" Bewertung der Rechtsordnung werden im Urteil des EuGH nicht formuliert. Sollten sich Verantwortliche oder Auftragsverarbeiter mit der Rechtsordnung des Empfängers im Drittland u.a. anhand des Art. 45 Abs. 2 DS-GVO auseinandergesetzt haben, ist Ziff. 7 mit „ja" zu beantworten. Informationen von konzernangeschlossenen Unternehmen können beispielsweise hierzu verwendet werden.

Folgefrage: Haben Sie dabei insbesondere überprüft, ob es in den Rechtsvorschriften des Drittlandes keine Bestimmungen gibt, die es den Empfängern unmöglich machen, ihren vertraglichen Verpflichtungen gemäß den SDK nachzukommen, um sicherzustellen, dass das im EWR garantierte Datenschutzniveau natürlicher Personen nicht untergraben wird?

Hinweise: Hier gelten die Ausführungen zu Ziff. 7.

Folgefrage: Sofern die (mögliche) Kenntnisnahme der personenbezogenen Daten in den USA erfolgt, unterfallen Sie oder ein Empfänger der Section 702 des Foreign Intelligence Surveillance Act (FISA) der USA, der US-Behörden Zugang zu den Daten bei Anbietern elektronischer Kommunikationsdienste ermöglicht?

Hinweise: Der Justizminister und der Direktor der nationalen Nachrichtendienste könnten gemäß Section 702 FISA nach Billigung durch den Foreign Intelligence Surveillance Court (FISC) gemeinsam zur Beschaffung von „Informationen im Bereich der Auslandsaufklärung" die Überwachung von Personen genehmigen, die keine amerikanischen Staatsbürger sind und sich außerhalb des Hoheitsgebiets der Vereinigten Staaten aufhalten. Die auf dieser Vorschrift gestützten Überwachungsprogramme hat der EuGH als unverhältnismäßig eingestuft, so dass an dieser Stelle in den Augen des Gerichts kein „in der Sache gleichwertiges" Datenschutzniveau besteht.

Hinweise zum Anwendungsbereich von Section 702 FISA sind beispielsweise einem Papier des Wissenschaftlichen Dienstes des Bundestages mit weiteren Verweisen zu entnehmen[5]. Mit Blick auf konzerninterne Datenimporteure sollten Informationen zum Geltungsbereich von Section 702 direkt bei der Tochter- oder Muttergesellschaft eingeholt werden können.

Frage 8: Wenn Sie zu dem Schluss gelangt sind, dass der Empfänger tatsächlich die Erfüllung der vertraglichen Verpflichtungen gemäß den SDK garantieren kann: Beschreiben Sie bitte Ihre Gründe für diese Schlussfolgerung im Einzelnen und erbringen Sie geeignete Nachweise.

Hinweise: Der EuGH hat Feststellungen zum angemessenen Datenschutzniveau für Empfänger personenbezogener Daten in den USA getroffen, die der Section 702 FISA unterliegen. Andere Empfänger in den USA oder in einem anderen Drittland waren nicht Bestandteil des Urteils. Die neuen Standarddatenschutzklauseln der Kommission enthält unter Klausel 14 (b) weiterführende Hinweise, wie eine Analyse der Übermittlung mit Blick auf die Rechtsordnung im Empfängerland ausgestaltet werden kann:

i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

[5] https://t1p.de/svxp

ii) 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,

iii) 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.

Sollten sich aus der Analyse keine Hinweise für die Nichteinhaltung der Standarddatenschutzklauseln ergeben, kann dieser Umstand als Antwort auf Frage 8 kommuniziert werden. Die Ergebnisse dieser Analyse können ebenfalls als „Gründe" für die Schlussfolgerung herangezogen werden. Die Dokumentation der Analyse sollte insoweit als Nachweis ausreichend sein, zumal sich weder aus den Standarddatenschutzklauseln noch aus dem Gesetz bspw. eine Pflicht zur Vorlage von Konformitätsbescheinigungen Dritter ergibt.

Frage 9: Wenn Sie zu dem Schluss gekommen sind, dass der Empfänger die Erfüllung der vertraglichen Verpflichtungen gemäß den SDK nicht garantieren kann: Welche zusätzlichen Maßnahmen im Sinne der oben genannten Entscheidung des Europäischen Gerichtshofs haben Sie unternommen?

Hinweise: Kann die Einhaltung der Standarddatenschutzklauseln durch den Datenimporteur nicht gewährleistet werden, muss der Datenexporteur zusätzliche Maßnahmen implementieren, um weiterhin personenbezogene Daten an ihn zu übermitteln. Der Europäische Datenschutzausschuss hat in seinen Empfehlungen 01/2020 Hinweise zu möglichen zusätzlichen Maßnahmen gegeben. Insoweit kommen grundsätzlich technische, organisatorische wie auch vertragliche Maßnahmen in Betracht.

Frage 10: Da sich die Rechtslage im Drittland ändern kann: Wie stellen Sie eine schnelle Reaktion und datenschutzkonforme Anpassung an neue Gegebenheiten sicher? Beschreiben Sie insbesondere den Melde- und den Reaktionsprozess zwischen Ihrem Unternehmen und dem Empfänger im Drittland.

Hinweise: An dieser Stelle ist die Kommunikation zwischen dem Datenexporteur und dem Datenimporteur hinsichtlich Änderungen der Rechtslage beim Datenimporteur zu beschreiben. Nicht jede Änderung der Rechtslage wird dem Datenexporteur gemeldet werden müssen, sondern nur solche, die sich nachteilig auf die Einhaltung der Standarddatenschutzklauseln auswirken können. In einem Konzernverbund wird besagter Austausch in der Regel von Vertretern der Rechtsabteilungen vorgenommen werden.

Frage 11: Werden die Daten nach Ziffer 1 und 2 verschlüsselt? Falls ja, beschreiben Sie bitte die Art der Verschlüsselung, in welchem Stadium des Informationsabrufs sie eingesetzt wird und in welchem Stadium und durch wen eine Entschlüsselung stattfindet. Bitte teilen Sie in dem Fall auch mit, welche Stellen über die Schlüssel verfügen. Geben Sie bitte auch an, ob die Verschlüsselung den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entspricht.

Hinweise: Die Empfehlungen 01/2020 des EDSA geben Hinweise darüber, welche Verschlüsselung in bestimmten Konstellationen eines Drittlands-transfers als angemessen erachtet wird.

Frage 12: Bitte nennen Sie auch vorbereitende Schritte im Hinblick auf ggf. noch nicht vollständig umgesetzte Maßnahmen nach Ziff. 9 bis Ziff. 11.

Keine weiteren Hinweise

Frage 13: Für den Fall, dass die Umstellung auf andere Systeme geplant ist, teilen Sie uns bitte die erwogenen Lösungen und den Stand der Umsetzung nebst Zeitplan für den Abschluss mit.

Keine weiteren Hinweise

Frage 14: Sofern Sie anstelle von SDK andere Übermittlungsinstrumente einsetzen, beantworten Sie bitte die Fragen 7 – 13 entsprechend (bitte Anlage beifügen).

Hinweise: Bei der Verwendung von Übermittlungsinstrumenten gem. Art. 46 DS-GVO muss die Frage der Effektivität der jeweiligen Garantie überprüft werden (vgl. Art. 46 Abs. 1 DS-GVO). Daher zielt diese Frage beispielsweise auf eine Analyse der Rechtsordnung im Empfängerland auch beim Einsatz von Binding Corporate Rules oder im Falle von Ad-hoc-Verträgen ab. Ausgenommen von einer Beantwortung sind gültige Angemessenheitsbeschlüsse der Kommission oder die Verwendung einer Ausnahme nach Art. 49 DS-GVO.

Frage 15: Bitte lassen Sie uns alle den konzerninternen Datenverkehr betreffenden Teile Ihres Verzeichnisses der Verarbeitungstätigkeiten zukommen, bei welchen es zu Datenübermittlungen in Drittländer kommt oder kommen kann.

Keine weiteren Hinweise

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de
www.gdd.de