Die Rolle von „Übereinkommen Nr. 108+“ im Rahmen der Prüfung des Datenschutzniveaus in Drittländern nach der DSGVO

Dr. Carlo Piltz, Philipp Quiel LL.M., 31.8.2020

Nach der Entscheidung des EuGH in der Rechtssache Schrems II (C-311/18) wird vermehrt deutlich, dass der Inhalt dieses Urteils bei weitem nicht nur Auswirkungen auf Datenübermittlungen in die USA hat. International tätige Unternehmen haben häufig auch Niederlassungen in datenschutzrechtlichen Drittländern, die wiederum zum Teil Mitglied des Europarates sind. Innerhalb von Unternehmensgruppen erfolgen regelmäßig Datenübermittlungen durch Zugriff auf Daten, die in Europa gespeichert sind, oder durch Übermittlung von Daten aus Europa an ein Unternehmen, das sich nicht in einem Mitgliedstaat befindet.

Für die Übermittlung von Daten in solche Drittländer gelten die Vorgaben aus Kapitel V DSGVO selbstverständlich auch. Letztendlich ist im Umkehrschluss zu der Aussage im zweiten Satz von Rn. 135 des EuGH-Urteils zu prüfen, ob das Recht eines Drittlandes dem Empfänger aus der Union übermittelter personenbezogener Daten keine Verpflichtungen auferlegt, die den vertraglichen Vereinbarung zwischen Exporteur und Importeur widersprechen und ob die vertraglichen Abmachungen nicht untergraben und eingehalten werden. Es stellt sich die Frage, welche Bedeutung das Übereinkommen Nr. 108+ (man spricht von „Nr. 108+“, da das alte Übereinkommen im Jahre 2018 angepasst wurde) des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) bei der Prüfung des Schutzniveaus in Drittländer spielt, die Vertragspartei dieses völkerrechtlichen Übereinkommens sind. Vertragsparteien des Abkommens können gemäß Art. 27 Abs. 1 nicht nur Mitglieder des Europarates sein, sondern auch andere „Nichtmitgliedstaaten“, die dazu eingeladen werden, dem Übereinkommen beizutreten.

A. Bedeutung geeigneter Garantien für Datenübermittlungen

Sofern für ein Land, Sektor oder Gebiet in einem Land kein Angemessenheitsbeschluss nach Art. 45 DSGVO besteht, sind vor allem geeignete Garantien nach Art. 46 DSGVO – und als solche Standardvertragsklauseln (SCC) – als Mechanismus für Übermittlungen relevant, die nicht nur gelegentlich erfolgen oder aus anderen Gründen nicht durch Art. 49 Abs. 1 DSGVO gerechtfertigt werden können. Im Hinblick auf die USA wird derzeit nach einer Antwort darauf gesucht, wie die Gretchenfrage nach passenden zusätzlichen Schutzmaßnahmen zu lösen ist, damit die SCC und andere geeigneten Garantien im Sinne von Art. 46 Abs. 2 DSGVO für die Übermittlung verwendet werden können.

Für Unternehmen ist vor allem problematisch, dass die nach Art. 46 Abs. 1 DSGVO erforderlichen „durchsetzbaren Rechte“ und „wirksamen Rechtsbehelfe“ maßgeblich von der Rechtsordnung im Drittland abhängig sind und deswegen in der Regel außerhalb des Einflussbereichs der datenverarbeitenden Parteien liegen. Zudem muss die Rechtsordnung des Drittlandes für zulässige Eingriffe erforderliche Einschränkungen und Garantien vorsehen (C-311/18, Rn. 168). In diesem Kontext ist für SCC auch die Fußnote zur Überschrift von Klausel 5 zu beachten. Der dort enthaltene Verweis auf Art. 13 Abs. 1 der RL 95/46 EG ist nun als Verweis auf Art. 23 DSGVO zu verstehen, anhand dessen im Recht des Drittlands vorgesehene Beschränkungen auf ihre Zulässigkeit überprüft werden müssen. Zwingende Erfordernisse des Rechts im Drittland, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft zur Gewährleistung u. a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist, widersprechen den SCC nicht (C-311/18, Rn. 141).

B. Prüfung des Schutzniveaus in einem Staat, der Vertragspartei des Übereinkommen Nr. 108+ ist

Der EuGH hat in Rn. 125 betont, dass die SCC und andere vertragliche Abmachungen zwischen Exporteur und Importeur staatliche Stellen nicht binden können, weil diese nicht Vertragspartei sind. Neben der Ebene von privatwirtschaftlichen Vereinbarungen zwischen Datenverarbeitern, sind aber unserer Auffassung nach bei der Suche und Prüfung eines gleichwertigen Schutzniveaus auch Verträge in den Blick zu nehmen, deren Vertragsparteien Staaten sind, die sich international Verpflichtungen auferlegen. Der erste völkerrechtlich verbindliche Vertrag mit datenschutzrechtlichem Inhalt ist das Übereinkommen Nr. 108. Die im Jahre 2018 angepasste Fassung des Übereinkommens ist sehr eng an der DSGVO und europäischen primärrechtlichen Datenschutznormen orientiert, offenbart jedoch auch Bezugspunkte zum Recht auf Achtung des Privat- und Familienlebens aus Art. 7 GRC und Art. 8 EMRK und zum Recht auf wirksame Rechtsbehelfe und ein unparteiisches Gericht aus Art. 47 GRC.

Bei der Prüfung des Schutzniveaus für Datenübermittlungen in ein Drittland, das Vertragspartei des Übereinkommen Nr. 108+ ist, drängt sich die Frage auf, welche Rolle die in diesem Übereinkommen geregelten Verpflichtungen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten spielen. Das in Art. 14 Abs. 1 normierte grundsätzliche Verbot der Untersagung von Datenübermittlungen in Länder, die Vertragspartei des Übereinkommen Nr. 108+ sind, und die in Art. 14 Abs. 2 und 3 geltenden Ausnahmen für Staaten, die nicht Vertragspartei des Übereinkommens sind, lassen stark vermuten, dass dem Übereinkommen Nr. 108+ eine große Rolle bei der Prüfung des Schutzniveaus in Vertragsstaaten zukommen kann. Zudem regelt Art. 14 Abs. 3 a), dass internationale Verträge und Vereinbarungen bei der Prüfung des Schutzniveaus in einem Drittland beachtet werden können. Dies spricht auch für eine Einbeziehung der Regelungen des Übereinkommen Nr. 108+ bei der Prüfung des Schutzniveaus in den Vertragsstaaten.

Gemäß Art. 1 des Übereinkommen Nr. 108+ ist der Zweck (hier in nicht offizieller Übersetzung ins Deutsche), *„jede Person, ungeachtet ihrer Staatsangehörigkeit oder ihres Wohnsitzes, bei der Verarbeitung ihrer personenbezogenen Daten zu schützen und damit zur Achtung ihrer oder seiner Menschenrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, beizutragen.* Zudem gilt nach Art. 4 Abs. 1 die Pflicht, dass *„jede Vertragspartei in ihrem Recht die erforderlichen Maßnahmen trifft, um die in diesem Übereinkommen aufgestellten Regelungen zu verwirklichen und ihre Wirksamkeit sicherzustellen*".

Im Folgenden werden einzelne Reglungen aus dem Übereinkommen Nr. 108+ jeweils spezifische Anforderungen an Übermittlungen in Drittländer gegenübergestellt. Hierbei werden sowohl allgemeine Vorgaben aus der DSGVO als auch speziell für Übermittlungen geltende Vorgaben beachtet. Die aktuelle Fassung des Übereinkommen Nr. 108+ gibt es in amtlicher Fassung bisher nur auf Englisch und Französisch. Im Folgenden wird daher auf die englische Fassung des Übereinkommen Nr. 108+ verwiesen.

Vorgaben	Regelungen im Übereinkommen Nr. 108+
Einhaltung der Datenschutzgrundsätze	**Article 5 – Legitimacy of data processing and quality of data** (1) **Data processing** shall be **proportionate** in **relation** to the **legitimate purpose** pursued and **reflect** at **all stages** of the processing **a fair balance between all interests** concerned, whether public or private, and the rights and freedoms at stake. (2) Each Party shall provide that **data processing can be carried** out on the **basis of the free, specific, informed and unambiguous consen**t of the data subject **or of some other legitimate basis laid down by law**. (3) Personal data undergoing processing shall be **processed lawfully**.

	(4) Personal data undergoing processing shall be: a) processed **fairly** and in a **transparent manner**; b) **collected** for **explicit, specified and legitimate purposes** and **not processed** in a way **incompatible with those purposes**; further **processing for archiving purposes** in the public interest, **scientific or historical research** purposes or **statistical** purposes is, subject to **appropriate safeguards**, compatible with those purposes; c) **adequate, relevant** and **not excessive** in **relation to the purposes** for which they are processed; d) **accurate** and, where necessary, **kept up to date**; e) **preserved** in a form which **permits identification of data subjects** for **no longer than** is **necessary** for the purposes for which those data are processed. **Article 10 – Additional obligations** (1) **Each Party shall provide** that **controllers** and, where applicable, **processors**, take all **appropriate measures to comply with the obligations of this Convention** and **be able to demonstrate**, **subject to the domestic legislation adopted** in accordance with Article 11, paragraph 3, in particular to **the competent supervisory authority** provided for in Article 15, that the data processing under their control **is in compliance with the provisions of this Convention**.
Besonderer Schutz besonderer Datenkategorien	**Article 6- Special categories of data** (1) The processing of: – genetic data; – personal data relating to offences, criminal proceedings and convictions, and related security measures; – biometric data uniquely identifying a person; – personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall **only be allowed** where **appropriate safeguards are enshrined in law**, complementing those of this Convention. (2) Such safeguards **shall guard against** the **risks** that the **processing of sensitive data may present** for the **interests, rights and fundamental freedoms of the data subjec**t, notably a **risk of discrimination**.
Datensicherheit und Meldung von Verletzungen der Sicherheit an die zuständige Aufsichtsbehörde	**Article 7 – Data security** (1) Each Party shall provide that the **controller**, and, where applicable the **processor**, **takes appropriate security measures** against risks such as **accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data**.

	(2) Each Party shall provide that the **controller notifies, without delay, at least the competent supervisory authority** within the meaning of Article 15 of this Convention, of **those data breaches** which **may seriously interfere with the rights and fundamental freedoms of data subjects**. **Article 10 – Additional obligations** (3) **Each Party shall provide** that **controllers**, and, where applicable, **processors**, **implement technical and organizational measures** which take into account the **implications of the right to the protection of personal data** at all stages of the data processing.
Informationspflichten	**Article 8 – Transparency of processing** (1) Each Party shall provide that the **controller informs the data subjects** of: a) his or her **identity** and **habitual residence or establishment**; b) the **legal basis** and the **purposes** of the intended processing; c) the **categories of personal data** processed; d) the **recipients or categories of recipients** of the personal data, if any; and e) the **means of exercising the rights set out in Article 9**, as well as **any necessary additional information** in order to **ensure fair** and **transparent processing** of the personal data.
Eingriffe in Rechte sind auf das zwingen Erforderliche beschränkt und gehen nicht über das hinaus, was in einer demokratischen Gesellschaft zur Gewährleistung u. a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist	**Article 8 – Transparency of processing** (2) **Paragraph 1** shall **not apply** where the **data subject already has the relevant information**. (3) Where the personal data **are not collected from the data subjects**, the controller shall **not be required** to provide such information where the processing **is expressly prescribed by law** or this **proves** to be **impossible or involves disproportionate efforts**. **Article 9 – Rights of the data subject** (2) **Paragraph 1.a** shall **not apply** if the decision is **authorised by a law** to which the controller is subject and which also **lays down suitable measures to safeguard the data subject's rights**, **freedoms and legitimate interests**. **Article 11 – Exceptions and restrictions** (1) **No exception to the provisions set out in this Chapter shall be allowed except** to the provisions of **Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9,** when **such an exception is provided for by law**, **respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:** a) the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and

	prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; b) the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression. (2) **Restrictions** on the **exercise of the provisions** specified in **Articles 8 and 9** may be provided for **by law** with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when **there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects**. (3) In addition to the exceptions allowed for in paragraph 1 of this article, with **reference to processing activities for national security** and **defense purposes**, each Party **may provide, by law** and **only to the extent that it constitutes a necessary and proportionate measure** in a **democratic society** to **fulfill such aim**, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d. This is **without prejudice** to **the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision** under the **domestic legislation** of the respective Party.
Durchsetzbare Rechte	**Article 9 – Rights of the data subject** (1) Every individual shall have a right: a) **not to be subject to a decision significantly affecting him or her based solely on an automated processing** of data **without having his or her views taken into consideration**; b) to **obtain, on request**, at **reasonable intervals** and **without excessive delay or expense**, **confirmation of the processing** of personal data relating to him or her, the **communication in an intelligible form** of the **data processed**, **all available information on their origin**, on the **preservation period** as well as **any other information** that the controller is **required to provide** in order to **ensure the transparency** of processing in accordance with **Article 8, paragraph 1**; c) to **obtain, on request**, **knowledge of the reasoning** underlying data processing **where the results** of such processing **are applied** to him or her; d) to **object at any time,** on **grounds relating to his or her situation, to** the **processing** of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms; e) to **obtain, on request**, **free of charge** and **without excessive delay**, **rectification or erasure**, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

	f) to have a **remedy under Article 12 where his or her rights under this Convention have been violated;** g) to **benefit, whatever** his or her **nationality or residence**, from the **assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention**.
Wirksame Rechtsbehelfe	**Article 1 – Object and purpose** The purpose of this Convention is to **protect every individual**, **whatever** his or her **nationality** or **residence**, with regard to the processing of their personal data, thereby **contributing to respect** for his or her **human rights** and **fundamental freedoms**, and in particular the **right to privacy**. **Article 3 – Scope** (1) Each Party undertakes **to apply this Convention** to **data processing subject to its jurisdiction** in the **public and private sectors**, thereby **securing every individual's right to protection** of his or her personal data. **Article 4 – Duties of the Parties** (3) Each Party undertakes: a) to **allow** the **Convention Committee** provided for in Chapter VI to **evaluate the effectiveness** of the **measures it has taken in its law** to **give effect to the provisions of this Convention**; and b) to **contribute actively to this evaluation** process. **Article 10 – Additional obligations** (4) Each Party may, having regard to the **risks arising** for **the interests, rights and fundamental freedoms of the data subjects**, adapt the application of the provisions of **paragraphs 1, 2 and 3** in **the law** giving **effect to the provisions of this Convention**, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor. **Article 12 – Sanctions and remedies** Each Party undertakes to establish a**ppropriate judicial and non-judicial sanctions** and **remedies** for violations of the provisions of this Convention.
Behörden, die Einhaltung der Vorgaben kontrollieren	**Article 15 – Supervisory authorities** (1) **Each Party shall provide** for **one or more authorities** to be **responsible for ensuring compliance** with the **provisions of this Convention**. *Anmerkung*: An dieser Stelle wurde aus Platzgründen auf den Abdruck der weiteren Vorgaben aus Art. 15 verzichtet. **Article 16 – Designation of supervisory authorities** (1) **The Parties agree to co-operate** and **render** each other **mutual assistance in order to implement this Convention**.

	Anmerkung: An dieser Stelle wurde aus Platzgründen auf den Abdruck der weiteren Vorgaben aus Art. 16 verzichtet.
Abschätzung und Beachtung des von einer Datenverarbeitung ausgehenden Risikos	**Article 10 – Additional obligations** (2) **Each Party shall provide** that **controllers** and, where applicable, **processors**, **examine the likely impact of intended data processing** on the **rights and fundamental freedoms of data subjects prior to** the **commencement** of such processing, and shall **design the data processing** in such a manner as to **prevent or minimise the risk of interference with those rights and fundamental freedoms**.

Alle Vertragsparteien verpflichten sich nach Art. 3 Abs. 1, das Übereinkommen auf die ihrer Hoheitsgewalt unterstehende Datenverarbeitung im öffentlichen und privaten Sektor anzuwenden und dadurch das Recht jedes einzelnen auf den Schutz seiner oder ihrer personenbezogener Daten zu gewährleisten. In der vorherigen Fassung Übereinkommen Nr. 108 war in Art. 3 Abs. 2 a) noch die Möglichkeit vorgesehen, dass einzelne Staaten das Übereinkommen auf bestimmte Arten von automatisierten Dateien und Datensammlungen mit personenbezogenen Daten nicht anwenden (vgl. hierzu diese Übersicht). Auf dieser Grundlage hatten einige Staaten beispielswiese erklärt, das Übereinkommen nicht auf Datenverarbeitungen anzuwenden, die von öffentlichen Einrichtungen zum Zwecke der nationalen Sicherheit, der Verteidigung sowie zur Ermittlung und Verhütung von Straftaten verarbeitet werden. Diese Möglichkeit, die Geltung des Übereinkommen Nr. 108+ auf bestimmte Bereiche nicht anzuwenden, gibt es in der Fassung aus 2018 nicht mehr.

c. Zusammenfassendes Fazit zur Bedeutung des Übereinkommen Nr. 108+

Der oben durchgeführte Vergleich offenbart, dass das Übereinkommen Nr. 108+ Vieles ausgleicht, was vom EuGH in Bezug auf die Rechtslage und das daraus ableitbare Schutzniveau in den USA moniert wurde. Insbesondere durchsetzbare Rechte und wirksame Rechtsbehelfe und ein Mindestmaß an Schutz personenbezogener Daten und Achtung des Privat- und Familienlebens sind umfangreich durch die völkerrechtliche Verpflichtung der Vertragsparteien im Übereinkommen Nr. 108+ sichergestellt. Dies wirkt sich bei der Prüfung des Schutzniveaus für ein Drittland unserer Auffassung nach sehr positiv aus und sollte bei der Prüfung durch Unternehmen in Bezug auf Vertragsstaaten unbedingt beachtet und dokumentiert werden. Klar ist aber auch, dass die USA kein Unterzeichner des Übereinkommen Nr. 108+ sind.