Handelskammer Hamburg

HAMBURG 2040
WIE WOLLEN WIR KÜNFTIG LEBEN - UND WOVON?

WHITEPAPER

HAMBURG 2040

WEGFALL PRIVACY SHIELD

Eine Orientierungshilfe für die Unternehmen Hamburgs

Vorwort

Am 16. Juli 2020 haben sich die datenschutzrechtlichen Rahmenbedingungen für viele Geschäftsprozesse von einem Tag auf den nächsten grundlegend geändert: Durch das Schrems-II-Urteil des Europäischen Gerichtshofs wurde eine regelmäßig genutzte datenschutzrechtliche Grundlage für die Übermittlung von personenbezogenen Daten in die USA mit sofortiger Wirkung entzogen. Damit müssen Unternehmen, die weitverbreitete Dienste wie etwa WhatsApp, YouTube, MS Teams, MS Office 365, Facebook, diverse Video-Konferenz-Tools u.v.m. nutzen, ihre Geschäftsprozesse und Dienstprogramme überprüfen und gegebenenfalls umstellen oder zusätzliche Schutzmaßnahmen für die übermittelten Daten ergreifen. Tun die Unternehmen dies nicht, verstoßen sie gegen geltendes Recht. Es können Kundenbeschwerden und hohe Strafen seitens der Aufsichtsbehörden drohen.

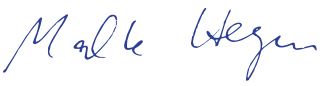
Für eine Vielzahl der Betriebe ist das eine große Herausforderung und löst dringenden Handlungsbedarf aus. Die Projektgruppe „Wegfall Privacy Shield" aus dem Handelskammer-Ausschuss für Informationstechnologie möchte Unternehmen bei der Bewältigung dieser Aufgabe unterstützen. Im ersten Schritt wurde ein Webinar organisiert, um Unternehmen für die Relevanz der Thematik und die eigene Betroffenheit zu sensibilisieren. Die Resonanz und der Klärungsbedarf waren sehr groß und die geäußerten Fragen der Teilnehmenden sind in das vorliegende Whitepaper eingeflossen. Es soll Unternehmen bei der notwendigen Prüfung der eigenen Geschäftsprozesse eine hilfreiche Unterstützung sein.

Dieses Whitepaper ist zudem mit Unterstützung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erarbeitet worden und stellt somit eine relevante Unterlage für Hamburger Unternehmen dar.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit befürwortet und unterstützt die hier beschriebene Vorgehensweise.

Handelskammer Hamburg

Prof. Norbert Aust
Präses



Dr. Malte Heyne
Hauptgeschäftsführer

Inhaltsverzeichnis

Glossar und Abkürzungsverzeichnis

BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
DS-GVO	Datenschutzgrundverordnung
edpb	European Data Protection Board
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
HmbBfDI	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit
SCC	Standardvertragsklauseln
SDK	Standarddatenschutzklauseln

I. Hintergrund und Zielsetzung

Der Vorteil des Privacy Shield war die Annahme eines adäquaten Datenschutzniveaus bei den Privacy-Shield-(selbst)zertifizierten Unternehmen ohne eine weitere Prüfung. In der Praxis bedeutete dies für Unternehmen, dass für die Übermittlung personenbezogener Daten in die USA keine gesonderten vertraglichen Übereinkommen oder Schutzmaßnahmen getroffen werden mussten. Seit Juli 2020 ist diese Regelung unwirksam. Unternehmen müssen nun aktiv werden und sich selbst umfänglich auf US- Datenübertragungen und deren rechtliche Grundlage hin überprüfen.

Das vorliegende Whitepaper gibt Hamburger Unternehmen allgemeine Handlungsempfehlungen zum Umgang mit dieser herausfordernden Situation, die gemeinsam mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit erarbeitet wurden. Diese Unterlage richtet sich an Unternehmen aller Größen und Branchen sowie Selbständige und Freelancer.

Wir empfehlen den Hamburger Unternehmen, sich grundsätzlich bei Problemen oder Verständnisfragen durch einen Rechtsanwalt oder einen Datenschutzberater unterstützen zu lassen. Eine Rechtsberatung wird hiermit ausdrücklich ausgeschlossen.

HINWEIS: *Diese Informationen sollen Ihnen nur erste Hinweise geben und erheben daher keinen Anspruch auf Vollständigkeit. Obwohl sie mit größtmöglicher Sorgfalt erstellt wurden, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden. Der Text kann eine umfassende Prüfung und Beratung durch einen Rechtsanwalt, Steuerberater oder die Auskunft durch die zuständige Behörde nicht ersetzen.*

1.1 IST Zustand

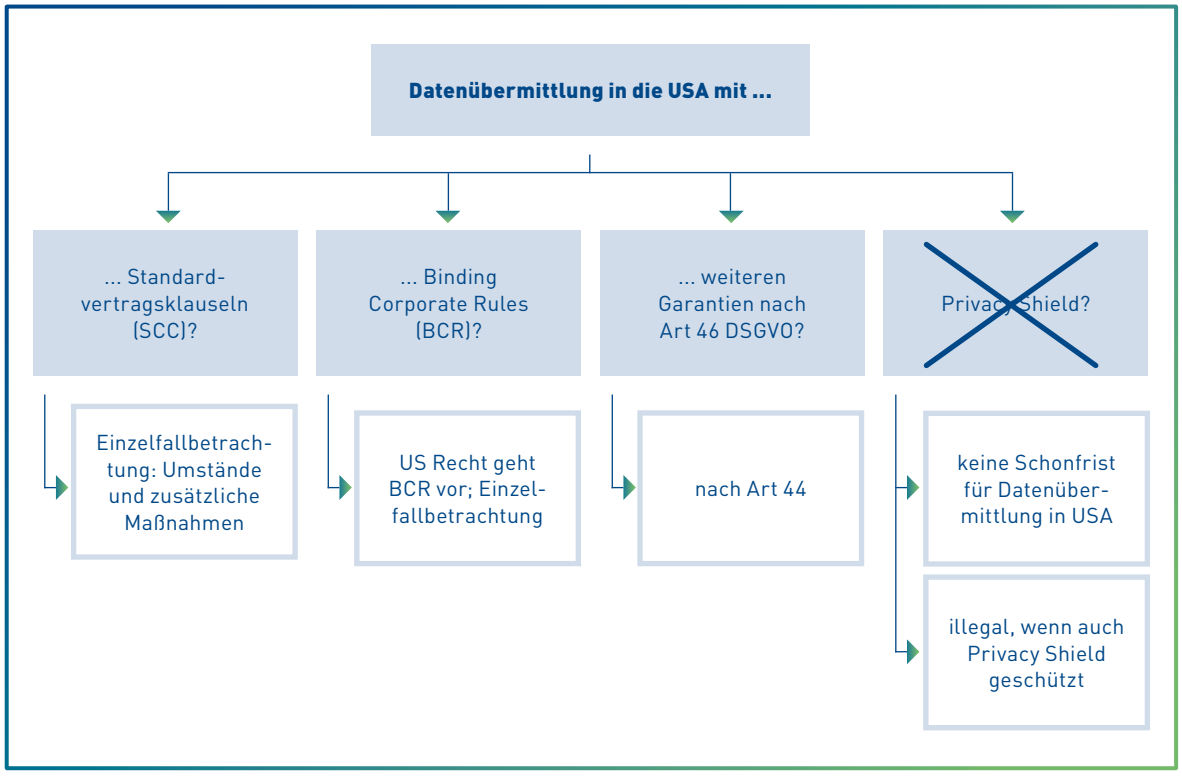
Für den Transfer personenbezogener Daten in Drittstaaten außerhalb der Europäischen Union (EU) gibt es eine Auswahl an Rechtsgrundlagen, auf die sich solche Datenübermittlungen stützen können (Abb. 1). Datentransfers in die USA basierten zuvor häufig auf einer dieser Rechtsgrundlagen, dem Privacy Shield Abkommen. Im Juli 2020 fiel diese Option mit sofortiger Wirkung weg.

Der Europäische Gerichtshof (EuGH) erklärte das EU-US-Privacy Shield mit seinem Urteil vom 16.07.2020 (Az: C 311/18) für ungültig und wies auf die Pflichten für Datenexporteure und -importeure bei Anwendung der EU-Standardvertragsklauseln, insbesondere hinsichtlich einer rechtskonformen Datenübermittlung, hin. Somit können nicht mehr auf Grundlage des Privacy Shields US-Server-Leistungen, Softwarelösungen, Videokonferenztools oder Cloud-Services genutzt werden. Unternehmen und Selbstständige (Datenexporteure) mit Sitz in der EU oder in Ländern des Europäischen Wirtschaftsraums (EWR) stehen nun vor der Herausforderung, wie personenbezogene Daten weiterhin rechtskonform in Drittländer übermittelt werden können.

1.2 SOLL Zustand

Unternehmen (Datenexporteure) mit Sitz in der EU oder im EWR sollen personenbezogene Daten wieder rechtskonform in die USA übermitteln können. Diese Unterlage soll eine Orientierung für Unternehmen zur Handhabung der momentanen Situation sein. Dazu sind die im Folgenden genannten Prüfschritte und Risikobewertungen vorzunehmen. Es müssen Maßnahmen erwogen und umgesetzt werden, um ein wirklich angemessenes Datenschutzniveau zu schaffen.

Abbildung 1: Übersicht der Rechtsgrundlagen für Datenübermittlung in die USA



II. Prüfschritte für Unternehmen[1]

Mit den folgenden Fragen sollen sich Unternehmen selbst testen. Die Ergebnisse sollten dokumentiert werden. Bei einer möglichen Überprüfung durch eine Aufsichtsbehörde empfehlen wir, dieses Prüfschema als Dokumentation und Nachweis der Unternehmensverantwortung sowie die Umsetzung der sich daraus ergebenden Maßnahmen einzureichen.

2.1 Ist mein Unternehmen vom Wegfall des Privacy Shields betroffen?

Prüfen Sie, ob Ihr Unternehmen grundsätzlich Datenübertragungen in Drittländer (außerhalb der EU) vornimmt. Nutzen Sie einen der hier beispielhaft aufgeführten Dienste, die sich auf den Privacy Shield stützen? (Dienste mit dem Serverstandort außerhalb EU) Z.B.:

- ◯ Gewerbliche Homepage mit Plug-Ins wie z.B. Google Maps
- ◯ Online Shops
- ◯ YouTube Einsatz
- ◯ WhatsApp Business
- ◯ Gewerbliches Social Media (z.B. Facebook, Twitter, Instagram, Linkedin ...)
- ◯ Live Chat Systeme
- ◯ Video Chat Systeme
- ◯ Video Konferenz Systeme
- ◯ Google Dienste
- ◯ Amazon Dienste
- ◯ Microsoft Dienste

Diese Liste ist beispielhaft. Die Betroffenheit bei konkreten Dienstleistungsprogrammen lässt sich jedoch nicht pauschal feststellen. Dazu ist immer die individuelle Situation des Unternehmens einzubeziehen. Wenn Sie einen oder mehrere dieser genannten Dienste in Ihrem Unternehmen nutzen, müssen Sie aktiv werden und die dadurch vorgenommenen Datenübermittlungen näher überprüfen sowie gegebenenfalls die in Frage kommenden Dienste auf Alternativen überprüfen. Beachten Sie hierzu unser Prüfschema „Zusätzliche Maßnahmen".

2.2 Prüfschema „zusätzliche Maßnahmen"

a) Welche Datenübermittlungen werden in den einzelnen Diensten vorgenommen?

- ◯ Personenbezogenen Daten z.B. Name, E-Mail-Adresse, postalische Adresse
- ◯ Besondere personenbezogene Daten, z.B. Eigenschaften, medizinische Daten
- ◯ Interne berufsbezogene Daten, die dem Betriebsgeheimnis unterliegen

b) Auf welcher Grundlage finden die Datenübermittlungen an den Datenverarbeiter statt?

- ◯ Server des Anbieters befindet sich innerhalb der EU, DSGVO konform
- ◯ Finden Datenübermittlungen Ihres Datenverarbeiters in die USA statt?
  - ◯ Standardvertragsklauseln (SCC)
  - ◯ Binding Corporate Rules (BCR)
  - ◯ Garantien nach Art 46 DSGVO
  - ◯ Keine davon- (bisher Privacy Shield)

c) Besteht ausreichender Schutz für die Daten?

Die Analyse ist ggf. mit Hilfe der "europäischen wesentlichen Garantien " vorzunehmen. Wenn Sie diese Frage nicht beantworten können, müssen weitere Informationen vom Datenverarbeiter dazu eingeholt werden.

- ◯ Ja
- ◯ Nein

d) Wenn Nein:

Prüfen Sie bitte, ob die Nutzung eines alternativen Dienstleistungsprogramms aus der EU und/oder mit rechtskonformer Datenübermittlung möglich ist.

e) Wenn für Ihr Unternehmen die Nutzung eines anderen Dienstleistungsprogramms nicht möglich ist, empfehlen wir, die Gründe schriftlich zu dokumentieren, und abzuwägen:

- ◯ Kritische Dienste weiter nutzen (Gefahr der Abmahnung und Sanktionen), oder
- ◯ kritische Dienste abschalten.

Es ist immer eine Einzelfallentscheidung für Sie und Ihr Unternehmen.

f) Regelmäßige Überprüfung und Evaluierung der gewählten Alternativen sowie der betreffenden Dienste.

1 Bei diesen Handlungsempfehlungen haben wir uns mit einem Prüfschema „zusätzliche Maßnahmen" zur Dokumentation der individuellen Unternehmenssituation an der offiziellen EMPFEHLUNG DES EDSA (Europäischer Datenschutz Ausschuss) für den Umgang mit der entstandenen Situation orientiert. Ebenso beziehen wir uns auf die Empfehlungen der „edpb" (European Data Protection Board) zu Maßnahmen zur Ergänzung von Übermittlungstools (Stand 10.11.2020).

2.3 Entscheidung für eine der grundsätzlich möglichen Handlungsoptionen

a) Die kritischen Dienste werden weiterverwendet. Hier bestehen Gefahren für Unternehmen und Selbstständige hinsichtlich Abmahnungen und Sanktionen.
b) Alternative Dienste suchen und verwenden (Überprüfung möglicher Risiken).
c) Die kritischen Dienste werden ein- bzw. abgestellt.

Alle drei Möglichkeiten müssen kritisch und sorgfältig von den Unternehmen geprüft werden. Hierbei müssen auch die Risiken überprüft werden, die durch die Verwendung der alternativen Dienste entstehen. Dafür ist eine Beurteilung der Eintrittswahrscheinlichkeit und des möglichen Schadensausmaßes notwendig.

HINWEISE DES HAMBURGISCHEN BEAUFTRAGTEN FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT:

Wie beurteilen Sie unseren Vorschlag zum Umgang der entstandenen Situation?
- *Es handelt sich um einen guten Überblick über die Problematik und die verbliebenen Handlungsoptionen. Die praktischen Schwierigkeiten werden im Detail liegen. Hier wird mit den eingesetzten Dienstleistern und gegebenenfalls unter Hinzuziehung externer Beratung zu ermitteln sein, welche Daten wohin fließen und wie dies unterbunden werden kann.*

Können Sie uns weitere Lösungsvorschläge/ Handlungsempfehlungen mitgeben?
- *Das erste Augenmerk sollte darauf gerichtet sein, sich nach Alternativen aus dem Europäischen Wirtschaftsraum umzusehen. Auch im Hinblick auf Geschäftsgeheimnisse kann kein Interesse daran bestehen, Territorien mit anlassloser Massenüberwachung einzubeziehen.*
- *Datenexporteure können unter Umständen mit ihren Betroffenen bzw. Kunden einen gemeinsam abgestimmten Weg gehen. Im Einzelfall – also nicht bei regelmäßigen Übermittlungen – kann es eine Lösung sein, sich die ausdrückliche Zustimmung des Betroffenen dafür zu holen, dass die Daten im Drittland verarbeitet werden dürfen. Zudem kann es in diesen Einzelfällen Konstellationen geben, in denen die Auslandsverarbeitung zur Vertragserfüllung notwendig ist. Das kann bei der Vertragsgestaltung zu berücksichtigen sein.*

III. Chancen und Risiken der (Nicht-)Umsetzung

Für den Fall einer möglichen Überprüfung durch eine Aufsichtsbehörde haben Sie eine Dokumentation der von Ihnen ergriffenen Prüfschritte und Maßnahmen. Zudem wird durch die Umsetzung der empfohlenen Prüfschritte eine strukturierte Dokumentation in den Unternehmen erzeugt, die zur Wettbewerbsfähigkeit und Qualitätssteigerung beiträgt. Sie schaffen damit eine bessere Übersicht der genutzten Dienstprogramme und des vorhandenen Datenaustausches im Unternehmen. Eine fundierte Entscheidungsfindung hinsichtlich der (weiterhin) genutzten Programme ist damit möglich.

Beachten Sie, dass die Informationsanfragen bei einzelnen Anbietern erfahrungsgemäß mit unterschiedlichen zeitlichen Verzögerungen verbunden sind. Außerdem können bei der Nutzung von alternativen Programmdiensten für Unternehmen Risiken bestehen und müssen daher im Einzelfall eingeschätzt und geprüft werden.

Bei der Nichtumsetzung der genannten Prüfschritte kann es zu Sanktionen seitens der Aufsichtsbehörde oder Schadenersatzforderungen der betroffenen Personen kommen. Wir empfehlen den Unternehmen, die ausgefüllte Liste der einzelnen Prüfschritte sowie die in Erwägung gezogenen und umgesetzten Maßnahmen zu dokumentieren.

IV. Aktuelle Entwicklungen und Ausblick

Da der Abschluss einer Nachfolgeregelung zum Privacy Shield im Moment noch nicht absehbar ist, muss schnellstens eine andere Vorgehensweise zur Legitimation personenbezogener Datenübermittlungen an Datenverarbeiter mit Sitz in den USA gemäß der Datenschutzgrundverordnung (DSGVO) gefunden werden.

Die EU-Kommission präsentierte Ende 2020 bereits einen Entwurf modernisierter Standardvertragsklauseln als möglichen Teilersatz des Privacy Shield. Es ist anzunehmen, dass die neuen Standarddatenschutzklauseln (SDK) im Juni/ Juli 2021 verabschiedet werden.

HINWEISE DES HAMBURGISCHEN BEAUFTRAGTEN FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT:

Wie beurteilen Sie grundsätzlich die entstandene Situation durch den Wegfall des Privacy Shield vor dem Hintergrund, dass die überarbeiteten SDK voraussichtlich Mitte des Jahres 2021 verabschiedet werden können?

- *An der Rechtssituation in den USA ändern auch die aktualisierten SDKs nichts, die Geheimdienste sind trotzdem aktiv und die Betroffenenrechte werden u.a. dadurch nicht gewahrt.*
- *Zusätzliche Maßnahmen zu den SDK sind nötig.*
- *Der Entwurf der neuen SDK ist ein Fortschritt gegenüber den bisherigen Fassungen, da er erweiterte Garantien zum Schutz europäischer Daten in Drittstaaten enthält. Jedoch können rein vertragliche Regelungen nichts an der anlasslosen Massenüberwachung in Drittstaaten ausrichten. Daher sind auch weiterhin technische Zusatzmaßnahmen notwendig, um Zugriffe in Drittstaaten zu unterbinden. Dies können vor allem kryptografische Maßnahmen (Verschlüsselung der Daten) beim Datenaustausch mit den USA zur Sicherstellung des Schutzes der Vertraulichkeit, Authentizität und/oder Integrität von Informationen sein.*
- *Auch im Datenaustausch mit anderen Drittländern (außer USA) muss es zusätzliche Maßnahmen geben.*

Welche wichtigen Quellen können die Hamburger Unternehmen für Ihre Information zum Thema zusätzlich nutzen?

- *Adressatengerechte Arbeitshilfen finden Sie u. a. bei den Kolleginnen und Kollegen vom Bundesbeauftragten für Datenschutz und Informationsfreiheit sowie aus Baden-Württemberg oder Niedersachsen*
- *Eine nahezu vollständige Übersicht über die behördlichen Praxishilfen finden Sie bei der Gesellschaft für Datenschutz und Datensicherheit.*

Diskutieren Sie mit! Finden Sie weitere Informationen zum Stand des Projekts, Ideen und Impulse für Hamburg im Jahr 2040 – und die Möglichkeit, sich einzubringen auf

www.hamburg2040.de

Herausgeber:
Handelskammer Hamburg | Adolphsplatz 1 | 20457 Hamburg
Postfach 11 14 49 | 20414 Hamburg | Telefon 040 36138-138
Fax 040 36138-270 | service@hk24.de | www.hk24.de

Projektkernteam aus dem Ausschuss für Informationstechnologie:
Kathrin Weber (IRM Interim-Risiko-Management GmbH)
Marcus Henschel (secion GmbH)
Carsten Ludowig (hamburg.de GmbH & Co. KG)
Elisabeth Weißbecker (Handelskammer Hamburg)
Dr. Michaela Ölschläger (Handelskammer Hamburg)

Mit freundlicher Unterstützung von:
Dr. Jens Ambrock (Referatsleiter Wirtschaft und Infrastruktur, HmbBfDI)

Juni 2021