

Frankfurt am Main, den 6. September 2023

**Offener Brief an Frau Präsidentin der Europäischen Kommission Ursula von der Leyen**

**Betreff: Kritische Beurteilung des Angemessenheitsbeschlusses C(2023) 4745 final vom 10.07.2023**

**Sehr geehrte Frau Präsidentin der Europäischen Kommission,**

die GMVV & Co. GmbH ist ein strategischer Think Tank, eingetragen beim Parlament der Europäischen Union und der Kommission im EU Transparency Register unter Sektion IV, der sich auf die Forschung im Bereich Strafrecht und Justiz in Verbindung mit dem Schutz der Menschen- und Bürgerrechte spezialisiert hat.

Der am 10.07.2023 gem. Art. 45 DSGVO verabschiedete Angemessenheitsbeschluss, der besagt, dass die USA einen angemessenen Datenschutz bieten, ist nicht mit der Charta der Grundrechte der Europäischen Union (EU-GrCh) zu vereinbaren. In Anerkennung der Prinzipien des EU-U.S. Data Privacy Frameworks (DPF) und der Executive Order (EO) 14086 zur Wahrung des Unionsrechts, kommen wir zu dem Entschluss, dass die Entscheidung der EU-Kommission in ihrer momentanen Fassung die Grundrechte auf Privatsphäre, Datenschutz und wirksamen Rechtsbehelf unverhältnismäßig einschränkt.

## I. Begründung

Die EU-Grundrechtecharta verpflichtet alle Organe und Einrichtungen der EU, die Grundrechte und Grundfreiheiten zu achten und zu wahren. Kommt der Europäische Gerichtshof (EuGH) zu dem Entschluss, dass eine Entscheidung eines EU-Organs nicht mit der Charta zu vereinbaren ist, wird diese Entscheidung für ungültig erklärt. So war es der Fall, als der EuGH im *Schrems I* Urteil 2015 und *Schrems II* Urteil 2020 die beiden Vorgänger des Data Privacy Frameworks, das Safe-Harbor-Abkommen und das Data Privacy Shield, für ungültig erklärte. Auf das letztere Urteil folgte eine Rechtsunsicherheit für Unternehmen bei dem unvermeidbaren Transfer von Personendaten zwischen der EU und den USA. Bisher wird dieser Rechtsunsicherheit mit Standardvertragsklauseln entgegengewirkt,<sup>1</sup> die für die Unternehmen einen erheblichen Mehraufwand bedeuten<sup>2</sup> und damit negative Auswirkungen auf die Wirtschaft mit sich ziehen. Vor diesem Hintergrund ist ein in Übereinstimmung mit den Grundfreiheiten und Grundrechten der EU geregelter und verständlicher Datenverkehr zwischen der EU und den USA nicht nur ein berechtigtes Interesse der EU-Bürger, sondern auch der EU-Unternehmen. Dabei muss ein wirksames und verständliches Rechtsschutzsystem durch die EU und die USA gewährleistet werden, das den Anforderungen der EU-Grundrechtecharta und der Europäischen Menschenrechtskonvention entspricht und im Hinblick auf ein faires Verfahren in Übereinstimmung steht mit den Leitentscheidungen des Europäischen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte.

### 1. Grundrecht auf Privatsphäre und Datenschutz

Die am 07.10.2022 verabschiedete Executive Order 14086 erweiterte das US-Datenschutzrecht und schränkte die Befugnisse der US-Nachrichtendienstbehörden ein,

---

<sup>1</sup> Ursula Sury, 'EU-U.S. Data Privacy Framework' [2023] Informatik Spektrum 46.

<sup>2</sup> IHK Region Stuttgart, 'Datenübermittlung in die USA und in Drittstaaten' (*ihk.de*, n.a.)

<<https://www.ihk.de/stuttgart/fuer-unternehmen/recht-und-steuern/datenschutzrecht/dateneubermittlung-usa-4852420?print=true&printsrc=button>> aufgerufen am 31.08.2023.

indem die Überwachungsmaßnahmen der US-Behörden, wie z. B. das PRISM-Programm der National Security Agency (NSA), fortan den Prinzipien aus Section 2(a) der EO 14086 folgeleisten müssen. Das heißt, US-Behörden dürfen nur solche Überwachungsmaßnahmen durchführen, die notwendig und verhältnismäßig sind, um eine „validierte nachrichtendienstliche[ ] Priorität“ voranzubringen.<sup>3</sup> Damit ist die Schranke, ab wann ein Überwachungsprogramm durchgeführt werden darf, mehr an den Wortlaut des Art. 52 EU-GrCh angepasst, als es bei dem Vorgänger der EO 14086, der Presidential Policy Directive 28 (PPD-28), noch der Fall war.<sup>4</sup> Trotz der wörtlichen Anpassung durch die Verwendung der Begriffe „notwendig“ und „verhältnismäßig“ innerhalb der EO 14086 sehen wir ein Problem bei der Auslegung der Begriffe. Es gibt keine Übereinstimmung der EU und den USA bezüglich einer expliziten Definition der genannten Begriffe und erfahrungsgemäß fällt die Auslegung von „verhältnismäßig“ und „notwendig“ im US-Recht und EU-Recht auseinander. Bereits in den Urteilen *Schrems I* und *Schrems II* wurde die fehlende Verhältnismäßigkeit der US-amerikanischen Massenüberwachungsprogramme wie dem o. g. PRISM-Programm oder dem Upstream-Programm bestimmt. Obwohl gemäß der EO 14086 die Individualüberwachung der Massenüberwachung als Mittel zur Informationsgewinnung vorgezogen werden muss,<sup>5</sup> liegt es im Ermessensspielraum der US-Behörden zu entscheiden, ab wann die Massenüberwachung ein notwendiges Mittel darstellt.

Im Ergebnis werden die Massenüberwachungsprogramme trotz der Executive Order 14086 weitestgehend unverändert weiterlaufen.<sup>6</sup> Somit werden Daten von EU-Bürgern seit Verabschiedung des Angemessenheitsbeschlusses legal von US-Behörden überwacht. Die von der EU-Kommission gestattete Legalisierung der Massenüberwachung von EU-Bürgern durch US-Behörden ist keine Verbesserung des

---

<sup>3</sup> Executive Order 14086, s 2(a)(ii)(A)(B).

<sup>4</sup> Maximilian Schrems, ‚New US Executive Order unlikely to satisfy EU law‘ (*noyb.eu*, 07.10.2022) <<https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>> aufgerufen am 31.08.2023.

<sup>5</sup> Executive Order 14086, s 2(c)(ii)(A).

<sup>6</sup> Executive Order 14086, s 2(c)(ii).

Rechtsschutzinteresses der EU-Bürger, sondern eine erhebliche Verschlechterung, die nicht in Übereinstimmung mit den rechtsstaatlichen Prinzipien der EU steht.

## 2. Keine Rechtsstaatlichkeit ohne angemessene Rechtsbehelfe

Auch wenn der Rechtsbehelfsmechanismus der EO 14086 eine deutliche Verbesserung gegenüber dem Ombudsverfahren des Data Privacy Shields darstellt, beispielsweise durch die Möglichkeit, die Löschung von unrechtmäßig gespeicherten Daten zu erwirken,<sup>7</sup> entspricht er noch nicht dem Schutzniveau des Art. 47 EU-GrCh. Das zweistufige Rechtsbehelfsverfahren sieht im ersten Schritt eine Überprüfung der möglichen Rechtsverletzung durch das Civil Liberties and Privacy Office (CLPO) vor und im Anschluss eine zweite Überprüfung durch den Data Protection Review Court (DPRC). Das Interesse des Beschwerdeführers wird dabei durch den sogenannten Special Advocat gesondert vertreten. Die Problematik dieses Verfahrens zeigt sich unter anderem in der fehlenden Transparenz. Die EO 14086 schreibt vor, dass Betroffene, unabhängig von den Ergebnissen der Überprüfungen des CLPO und des DPRC, nicht über eine Überwachung durch US-Behörden informiert werden.<sup>8</sup> Somit sind die Entscheidungen des CLPO und DRPC Verschlussache und weder der Öffentlichkeit noch dem Beschwerdeführer direkt zugänglich.<sup>9</sup>

Ferner ist die Unabhängigkeit des DPRC infrage zu stellen, da dieser, wie auch sein Vorgänger, als Teil der Exekutiven anzusehen ist und nicht als unabhängiges Gericht.<sup>10</sup> Die tatsächliche Wirksamkeit des Rechtsbehelfs wird in den kommenden Monaten genau beobachtet werden müssen. Die Webseite *dataprivacyframework.gov* der International Trade Administration und des U.S. Department of Commerce dient unter

---

<sup>7</sup> Executive Order 14086, s (4)(a).

<sup>8</sup> Executive Order 14086, s 3(c)(iii)(E), s 3(d)(i)(H).

<sup>9</sup> Europäisches Parlament, Entschließungsantrag zur Angemessenheit des vom Datenschutzrahmen zwischen der EU und den USA gebotenen Schutzes [2023] 2023/2501(RSP), Nr. 8.

<sup>10</sup> Europäisches Parlament, Entschließungsantrag zur Angemessenheit des vom Datenschutzrahmen zwischen der EU und den USA gebotenen Schutzes [2023] 2023/2501(RSP), Nr. 9.

anderem der Unterstützung von EU-Bürgern beim Einreichen von Beschwerden über Datenmissbrauch. Eine vergleichbare Plattform sollte auch auf EU-Ebene erstellt werden, um das Beschwerdeverfahren verständlich und durchführbar zu machen und es allen EU-Bürgern zu ermöglichen.

## II. Fehlende Übereinstimmung mit den Leitentscheidungen

Vor diesem Hintergrund kann man objektiv nur zu dem Schluss kommen, dass die erheblichen Beanstandungen des EuGH in den Urteilen *Schrems I* und *Schrems II* nicht ausreichend beachtet und umgesetzt wurden. Auch unter dem DPF werden die Rechte auf Achtung des Privat- und Familienlebens (Art. 7 EU-GrCh) und auf Schutz der personenbezogenen Daten (Art. 8 EU-GrCh) bei Übermittlung von Daten in die USA unverhältnismäßig eingeschränkt. Darüber hinaus ist der in der Executive Order 14086 vorgestellte Rechtsbehelfsmechanismus für EU-Bürger in Form des Data Protection Review Court und Special Advocats nicht ausreichend, um das Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht gem. Art. 47 EU-GrCh zu erfüllen. Im Ergebnis sehen wir die Ungültigkeit der momentanen Fassung des Angemessenheitsbeschlusses vor dem Europäischen Gerichtshof als unausweichlich an.

## III. Zusammenfassung

Abschließend fordern wir die EU-Kommission auf, die hier aufgeworfenen, erheblichen Rechtsmängel zu überprüfen und die rechtliche Grundlage für den transatlantischen Datentransfer so anzupassen und zu verbessern, dass die EU-Grundrechte und die Grundsätze eines fairen, transparenten und rechtsstaatlichen Verfahrens in Übereinstimmung mit der Grundrechtecharta, der EMRK und den einschlägigen Leitentscheidungen gewährleistet werden.

Wir fordern die EU-Kommission und das Europäische Parlament auf, den EU-U.S. Data Privacy Framework und den damit einhergehenden Datentransfer davon abhängig zu machen, dass die Daten von EU-Bürgern nicht durch geheime, intransparente oder anlasslose US-Massenüberwachungsprogramme erfasst werden.

Wir fordern die EU-Kommission dazu auf, dass die Begriffe „Notwendigkeit“ und „Verhältnismäßigkeit“ im Zusammenhang mit der Übertragung von Daten in einem bilateralen Abkommen, sowohl inhaltlich als auch formell und in Art und Umfang, definiert werden.

Wir fordern die EU-Kommission dazu auf, unverzüglich eine Monitoring-Einrichtung zu schaffen, welche die Aufgabe hat, die im Rahmen des Data Privacy Framework etablierten Rechtsbehelfsmechanismen in Bezug auf ihre Praktikabilität und tatsächliche Wirksamkeit zu überwachen. Die Ergebnisse der Überwachung sollen in einem jährlichen Bericht veröffentlicht werden. Die Berichte sollen als Grundlage dienen, notwendige Veränderungen und Verbesserungen des Data Privacy Frameworks vorzunehmen.

Wir fordern die EU-Kommission dazu auf, eine Übersetzung der Beschwerdewebseite ([dataprivacyframework.gov](https://dataprivacyframework.gov)) im Rahmen des Data Privacy Frameworks in alle 24 amtlichen EU-Sprachen zu veranlassen.

**GMW & Co. GmbH Think Tank**

Bergesgrundweg 3  
60599 Frankfurt am Main  
Germany  
T +49 (0)69 68091920  
F +49 (0)69 68091948

Kontakt:

**Dr. Michele Sciorba, LL.M. (Liverpool)**

Managing Director  
sciorba@gmvv.eu

**Liam Grunsky, LL.B.**

Wissenschaftlicher Mitarbeiter  
grunsky@gmvv.eu

**UnterzeichnerInnen**

Dr. Michele Sciorba, LL.M. (Liverpool), Managing Director GMVV & Co. GmbH Think Tank

Nicole Thamm, Managing Director GMVV & Co. GmbH Think Tank

Sarah Schuster, Leiterin Researchabteilung GMVV & Co. GmbH Think Tank

Michael Detjen, ehemaliges Mitglied EU-Parlaments, Berater für soziale Angelegenheiten  
GMVV & Co. GmbH Think Tank

Liam Grunsky, wissenschaftlicher Mitarbeiter GMVV & Co. GmbH Think Tank

Herr Rechtsanwalt Oliver Wallasch, Patron NGO Fair Trials International, Juristischer  
Berater GMVV & Co. GmbH Think Tank

Herr Rudolf Tillig, SPD-Politiker, ehemaliger, stellvertretender Vorsitzender der SPD-  
Betriebsgruppe Flughafen Frankfurt am Main

Frankfurt am Main, September 6, 2023

**Open Letter to Madam President of the European Commission Ursula von der Leyen**

**Subject: Critical assessment of the adequacy decision C(2023) 4745 final of 10 July 2023.**

**Dear Madam President,**

GMVV & Co. GmbH is a strategic Think Tank, registered with the Parliament of the European Union and the Commission in the EU Transparency Register under Section IV, specializing in research in the field of criminal law and justice in connection with the protection of human and civil rights.

The adequacy decision adopted on 10 July 2023 pursuant to Art. 45 GDPR, which states that the U.S. provides adequate data protection for the transfer of personal data to third-party countries, is incompatible with the Charter of Fundamental Rights of the European Union (CFR). Based on the principles of the EU-U.S. Data Privacy Framework (DPF) and Executive Order (EO) 14086, we conclude that the EU Commission's decision, as currently drafted, disproportionately restricts the fundamental rights to privacy, data protection, and effective remedy.



## I. Justification

The EU Charter of Fundamental Rights obliges all EU institutions and bodies to respect and uphold fundamental rights and freedoms. If the European Court of Justice (ECJ) concludes that a decision of an EU institution is not compatible with the Charter, this decision is invalid. This was the case when the ECJ declared the two predecessors of the Data Privacy Framework, the Safe Harbor agreement and the Data Privacy Shield, invalid in the 2015 *Schrems I* and 2020 *Schrems II* rulings, respectively. The latter ruling resulted in legal uncertainty for companies involved in the transfer of personal data between the EU and the US. So far, this legal uncertainty has been addressed using standard contractual clauses,<sup>11</sup> which requires considerable additional effort for companies<sup>12</sup> and has a negative impact on the economy. Against this background, data traffic between the EU and the U.S. that is regulated in accordance with the fundamental EU freedoms and rights is not only a legitimate interest of EU citizens, but also of EU companies. In this context, an effective and understandable system of legal protection must be ensured by the EU and the U.S. that meets the requirements of the EU Charter of Fundamental Rights and the European Convention on Human Rights and which is in line with the leading decisions of the European Court of Justice and the European Court of Human Rights with regard to procedural fairness.

### 1. Fundamental right to privacy and data protection

The passage of the Executive Order 14086 on 7 October 2022 expanded U.S. privacy law and limited the authority of U.S. intelligence agencies by requiring U.S. surveillance activities, such as the National Security Agency's (NSA) PRISM program, to follow the principles set forth in Section 2(a) of EO 14086. These principles state that U.S. agencies may only conduct surveillance activities that are necessary and proportionate

---

<sup>11</sup> Ursula Sury, 'EU-U-S. Data Privacy Framework' [2023] Informatik Spektrum 46.

<sup>12</sup> IHK Region Stuttgart, 'Datenübermittlung in die USA und in Drittstaaten' (*ihk.de*, n.a.)

<<https://www.ihk.de/stuttgart/fuer-unternehmen/recht-und-steuern/datenschutzrecht/datenuebermittlung-usa-4852420?print=true&printsrc=button>> accessed 31 August 2023.

to advance a “validated intelligence priority”.<sup>13</sup> Thus, the threshold for when a surveillance program may be conducted is more aligned with the wording of Article 52 of the CFR compared to EO 14086’s predecessor, Presidential Policy Directive 28 (PPD-28).<sup>14</sup> Despite this literal alignment, by using the terms “necessary” and “proportionate”, we see a problem with the interpretation of the terms. There is no agreement between the EU and the U.S. on an explicit definition of these terms, and experience shows that there are divergent interpretations of them in U.S. and EU law. The lack of proportionality of the U.S. mass surveillance programs such as the PRISM program or the Upstream program was determined in the *Schrems I* and *Schrems II* rulings. Although according to EO 14086 individual surveillance must be preferred over mass surveillance as a means of obtaining information,<sup>15</sup> it is up to the discretion of the U.S. authorities to decide at what point mass surveillance is a necessary means.

As a result, mass surveillance programs will continue largely unchanged despite Executive Order 14086.<sup>16</sup> Thus, data of EU citizens have been legally monitored by U.S. authorities since the adoption of the adequacy decision. The legalization of mass surveillance of EU citizens by U.S. authorities allowed by the EU Commission is not an improvement but a significant deterioration of the legal protections and interests of EU citizens that is not in accordance with the rule of law principles of the EU.

## 2. No rule of law without adequate legal remedies

Even though the appeal mechanism of EO 14086 represents a significant improvement over the ombudsman procedure of the Data Privacy Shield, for example through the possibility of obtaining the deletion of unlawfully stored data,<sup>17</sup> it does not yet meet the level of protection of Art. 47 CFR. The two-stage appeal procedure allows for a review

---

<sup>13</sup> Executive Order 14086, s 2(a)(ii)(A)(B).

<sup>14</sup> Maximilian Schrems, ‘New US Executive Order unlikely to satisfy EU law’ (*noyb.eu*, 7 October 2022) <<https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law>> accessed 31 August 2023.

<sup>15</sup> Executive Order 14086, s 2(c)(ii)(A).

<sup>16</sup> Executive Order 14086, s 2(c)(ii).

<sup>17</sup> Executive Order 14086, s (4)(a).

of the possible infringement of rights by the Civil Liberties and Privacy Office (CLPO) and then a second review by the Data Protection Review Court (DPRC). The complainant's interest is represented separately by the so-called Special Advocate. One of the problems with this procedure is the lack of transparency. EO 14086 stipulates that data subjects will not be informed of any monitoring by U.S. authorities, regardless of the results of the CLPO and DPRC reviews.<sup>18</sup> Thus, the decisions of the CLPO and DRPC are considered classified information and hence not directly accessible to the public or the complainant.<sup>19</sup>

Furthermore, the independence of the DPRC is compromised, since it, like its predecessor, is considered part of the executive branch and not an independent court.<sup>20</sup> The actual effectiveness of the appeal will have to be closely monitored in the coming months. The *dataprivacyframework.gov* website of the International Trade Administration and the U.S. Department of Commerce serves, among other things, to help EU citizens file complaints about data misuse. A comparable platform should be established at EU level in order to make the complaints procedure comprehensible and available for all EU citizens.

## II. Lack of conformity with the leading decisions

Against this background, we conclude that the significant objections of the ECJ in the *Schrems I* and *Schrems II* rulings have not been adequately implemented. Additionally, under the DPF, legal rights for the respect of private and family life (Art. 7 CFR) and protection of personal data (Art. 8 CFR), are disproportionately restricted when data are transferred to the US. Furthermore, the redress mechanism for EU citizens presented in Executive Order 14086, in the form of the Data Protection Review Court and Special Advocates, fails to ensure the right to an effective remedy and an impartial tribunal

---

<sup>18</sup> Executive Order 14086, s 3(c)(iii)(E), s 3(d)(i)(H).

<sup>19</sup> European Parliament, Motion for a resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework [2023] 2023/2501(RSP), no. 8.

<sup>20</sup> European Parliament, Motion for a resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework [2023] 2023/2501(RSP), no. 9.

guaranteed under Art. 47 CFR. As a result, we see it as inevitable that the current version of the adequacy decision will be ruled invalid by the European Court of Justice.

### III. Summary

In conclusion, we call on the EU Commission to review the significant legal deficiencies we have raised here and to adapt and improve the legal basis for transatlantic data transfers to ensure EU fundamental rights and the principles of a fair, transparent and constitutional process in accordance with the Charter of Fundamental Rights, the ECHR and the relevant leading decisions.

We call on the EU Commission and the European Parliament to make the EU-U.S. Data Privacy Framework and the accompanying data transfer conditional on the requirement that the data of EU citizens shall not be collected through secret, non-transparent or warrantless U.S. mass surveillance programs.

We call on the EU Commission to clearly define the nature and scope of the terms “necessity” and “proportionality” in the context of data transmission in a bilateral agreement.

We call on the EU Commission to immediately establish a monitoring body charged with the task of monitoring the practicality and effectiveness of the redress mechanisms established under the Data Privacy Framework. The results of the monitoring should be published in an annual report. These reports should serve as a basis for making necessary changes and improvements to the Data Privacy Framework.

We call on the EU Commission to initiate a translation of the complaint’s website (*dataprivacyframework.gov*) under the Data Privacy Framework into all 24 official EU languages.

**GMVV & Co. GmbH Think Tank**

Bergesgrundweg 3  
60599 Frankfurt am Main  
Germany  
T +49 (0)69 68091920  
F +49 (0)69 68091948

Contact:

**Dr. Michele Sciorba, LL.M. (Liverpool)**

Managing Director  
sciorba@gmvv.eu

**Liam Grunsky, LL.B.**

Research Associate  
grunsky@gmvv.eu

**Signatories**

Dr. Michele Sciorba, LL.M. (Liverpool), Managing Director GMVV & Co. GmbH Think Tank

Nicole Thamm, Managing Director GMVV & Co. GmbH Think Tank

Sarah Schuster, Head of Research GMVV & Co. GmbH Think Tank

Michael Detjen, Former Member EU-Parliament, Social Affairs Consultant GMVV & Co.  
GmbH Think Tank

Liam Grunsky, LL.B., Research Associate GMVV & Co. GmbH Think Tank

Attorney at Law Oliver Wallasch, Patron NGO Fair Trials International, Legal Advisor GMVV  
& Co. GmbH Think Tank

Rudolf Tillig, SPD-Politician, Former Vize-Chairman of the SPD Operation Group at Airport  
Frankfurt