privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Übermittlung von Personendaten an Organisationen in den USA auf der Grundlage des Swiss-US Data Privacy Framework

1 Zusammenfassung

Private Organisationen, die gemäss dem zwischen der Schweiz und den USA geltenden Data Privacy Framework (Swiss-U.S. DPF)[1] zertifiziert sind, haben ein angemessenes Datenschutzniveau.

Privatim gibt für kantonale und kommunale öffentliche Organe folgende drei Empfehlungen im Zusammenhang mit der Auslagerung von Daten an zertifizierte Organisationen ab:

1. **Verifizieren**: Zum Zeitpunkt einer geplanten Übermittlung von Personendaten an eine private Organisation in den USA ist die Rechtslage im Bereich des Swiss-US DPF zu verifizieren (https://www.dataprivacyframework.gov/list);
2. **Gütigkeit Zertifikat**: Es ist zu beachten, dass der Widerruf oder die Nichterneuerung des Zertifikats durch die Datenempfängerin jederzeit möglich ist;
3. **Ausstiegsszenario**: Bei einer Auslagerung der Bearbeitung von Personendaten an eine nach Swiss-U.S. DPF zertifizierte Organisation sind Ausstiegsszenarien zu planen.

2 Ausgangslage

Mit Verordnung vom 14. August 2024 hat der Bundesrat unter Vorbehalt die USA in die im Anhang 1 der Datenschutzverordnung (DSV; SR 235.11) aufgeführte Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe aufgenommen, in denen ein angemessenes Datenschutzniveau gewährleistet ist.[2] Der Vorbehalt lautet dahingehend, dass ein angemessenes Schutzniveau im Bereich des Datenschutzes i.S.v. Art. 16 Abs. 1 DSG (SR 235.1) nur privaten Organisationen bescheinigt wird, die gemäss des zu diesem Zeitpunkt zwischen der Schweiz und den USA geltenden Data Privacy Framework (Swiss-U.S. DPF)[3] zertifiziert sind. Bei der Zertifizierung i.S. des Swiss-US DPF handelt es sich um eine jährlich zu erneuernde Selbstzertifizierung der betreffenden privaten

---

1 Abrufbar unter https://www.dataprivacyframework.gov/EU-US-Framework => Switzerland, (Stand 3. März 2025).

2 Verordnung über den Datenschutz (Datenschutzverordnung, DSV), Änderung vom 14. August 2024, AS 2024 435.

3 Abrufbar unter https://www.dataprivacyframework.gov/EU-US-Framework => Switzerland, (Stand 3. März 2025).

privatim
c/o Datenschutzbeauftragter des Kantons Bern
Poststrasse 25, 3072 Ostermundigen
Tel. +41 (31) 633 74 10
praesident@privatim.ch, www.privatim.ch

Organisation gemäss Kapitel 3 Ziff. 6 Swiss-U.S. DPF. Eine Liste der zertifizierten Organisationen ist online einsehbar.[4]

Ein weiterer Grund für die Angemessenheitsbescheinigung bildet die Durchführungsverordnung (Executive Order; EO) 14086 vom 7. Oktober 2022. Hierbei handelt es sich um eine verbindliche Anweisung des Präsidenten, welche die Aufgabenerfüllung durch die Exekutive regelt. Konkret führt EO 14086 gewisse Massnahmen zur Verbesserung des Rechtsschutzes gegenüber Nachrichtendiensten ein. Insbesondere sieht es für Personen aus qualifizierten Staaten ein zweistufiges Beschwerdeverfahren vor.[5] Das Beschwerdeverfahren ermöglicht eine Überprüfung der Erhebung von Personendaten durch Nachrichtendienste in Bezug auf die Einhaltung von US-amerikanischem Recht durch den Civil Liberties Privacy Officer sowie den Data Protection Review Court. Beiden Instanzen wird durch die EO 14086 eine gewisse personelle und materielle Unabhängigkeit garantiert.[6]

Die Bescheinigung eines angemessenen Datenschutzes für zertifizierte Firmen nach dem Swiss-U.S. DPF dient als Grundlage für eine Datenbekanntgabe ins Ausland i.S.v. Art. 16 DSG und ist für Bundesorgane sowie Private verbindlich. Materiell-rechtlich stellt sie eine pauschalisierte Risikobeurteilung durch den Bundesrat dar, aufgrund derer die Übermittlung von Personendaten zwischen der Schweiz und den USA ohne weitere datenschutzrechtliche Garantien seitens der Empfängerin erfolgen darf.

Für öffentliche Organe der Kantone und Gemeinden ist die Bescheinigung nicht immer direkt rechtlich verbindlich, gilt aber im allgemeinen als genügende Grundlage für die Anerkennung eines angemessenen Datenschutzniveaus für Bekanntgaben sowie als ein mögliches Kriterium für die Datenschutz-Folgenabschätzung für grenzüberschreitende Auslagerungen von Datenbearbeitungen. Indessen bleiben öffentliche Organe von Kantonen und Gemeinden rechtlich für die entsprechende Risikoeinschätzung im Einzelfall verantwortlich.

3 Rechtsfolgen der Zertifizierung

3.1 Erleichterte Bekanntgabe von Personendaten an zertifizierte Firmen

Durch die Zertifizierung erklärt sich eine private Organisation als verpflichtet, bei der Bearbeitung von Personendaten, welche ihr gegenüber aus der Schweiz bekanntgegeben werden, die Prinzipien des Swiss-U.S. DPF einzuhalten. Hierbei handelt es sich um die nachfolgend aufgelisteten primären Prinzipien in Abschnitt II des Swiss-U.S. DPF, die ihrerseits durch weitere Prinzipien in Abschnitt III ergänzt werden.

- *Notice*. Eine weitreichende Informationspflicht, welche u.a. die Zertifizierung der Organisation sowie weiterer Unterorganisationen, die Verpflichtung zur Einhaltung der

---

4 Abrufbar unter https://www.dataprivacyframework.gov/list, (Stand 3. März 2025).

5 Die Schweiz wurde mit Schreiben des US-Generalstaatsanwalts vom 7. Juni 2024 und gestützt auf die Anerkennung eines angemessenen Datenschutzniveaus durch den Bundesrats als ein solchermassen qualifizierter Staat anerkannt, abrufbar unter https://www.justice.gov/opcl/media/1355326/dl?inline (Stand 4. März 2025).

6 Siehe die Erläuterungen in BUNDESAMT FÜR JUSTIZ, Beurteilung der Angemessenheit – Vereinigte Staaten Schaffung eines Datenschutzrahmens für die Übermittlung von Personendaten von der Schweiz an zertifizierte Organisationen in den Vereinigten Staaten (Swiss-U.S. Data Privacy Framework) – Beurteilung der Angemessenheit des Datenschutzes, S. 25 ff., abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/89019.pdf (Stand 4. März 2025).

Datenschutzprinzipien, den Erhebungszweck der Personendaten, die Rechte der Betroffenen, die Ansprechpersonen zur Wahrnehmung dieser Rechte, die designierte, kostenlose und unabhängige Streitbeilegungsinstanz, die Möglichkeit einer verbindlichen Arbitration sowie die Haftung für unrechtmässige Bekanntgaben an Dritte beinhaltet.

- *Choice*. Betrifft das Erfordernis der Einwilligung sowie deren rechtliche Anforderungen für die Weitergabe der Daten an Dritte oder für Zweckänderungen.
- *Accountability for Onward Transfer*. Regelt die Voraussetzungen für eine Bekanntgabe an Dritte unter Hinweis auf die ersten beiden Prinzipien sowie die Einhaltung der Zweckbindung und der Garantie eines gleichwertigen Datenschutzniveaus durch den Dritten.
- *Security*. Betrifft den Grundsatz der Datensicherheit sowie eine Beurteilung anhand der Risiken, die sich durch die Art und Weise der Bearbeitung sowie die Art der Personendaten ergibt.
- *Data Integrity and Purpose Limitation*. Umschreibt die Grundsätze der Datenminimierung sowie Aspekte der Datenrichtigkeit in Bezug auf den Bearbeitungszweck. Insbesondere enthält das Prinzip auch eine zeitliche Komponente, welche darauf hinausläuft, dass der Personenbezug von nicht mehr benötigten Daten aufgehoben werden muss. Das Prinzip steht unter dem Vorbehalt entgegenstehender Bearbeitungsinteressen wie der Bearbeitung im öffentlichen Interesse oder im Rahmen von Journalismus oder Kunst.
- *Access*. Datenschutzrechte auf Auskunft über die vorhandenen eigenen Personendaten sowie gegebenenfalls deren Änderung oder Löschung.
- *Recourse, Enforcement and Liability*. Pflicht zur Bereitstellung von wirksamen Mechanismen zur Sicherstellung der Einhaltung dieser Prinzipien.

Die Zertifizierung hat im Zusammenspiel mit dem durch die im Angemessenheitsbeschluss des Bundesrates genannten Rechtsgrundlagen geschaffenen regulatorischen Umfeld zur Folge, dass der betreffenden Organisation ein angemessenes Datenschutzniveau für die grenzüberschreitende Bekanntgabe von Personendaten bescheinigt wird. Dies ermöglicht eine Datenbekanntgabe an diese Organisation in den USA gestützt auf Art. 16 Abs. 1 DSG.

3.2 Auslagerung von Datenbearbeitungen an zertifizierte Firmen

Der Angemessenheitsbeschluss des Bundesrates entfaltet für Auslagerungen von Datenbearbeitungen – sowohl klassisch als auch in eine Cloudumgebung – nicht dieselbe Rechtswirkung wie für Datenbekanntgaben ins Ausland. Der Grund hierfür liegt darin, dass das auslagernde öffentliche Organ nach wie vor verantwortlich i.S. des Datenschutzrechts bleibt. Dies hat zur Folge, dass die Übermittlung der Daten, die notwendigerweise auch für eine Auslagerung erfolgen muss, grundsätzlich möglich ist, während zugleich eine Datenbearbeitung durch die Empfängerin zum Zweck der Aufgabenerfüllung des übermittelnden öffentliche Organs vertraglich geregelt werden muss.

Auf diese vertragliche Regelung sind die üblichen Vorschriften des Datenschutzrechts anwendbar, wie sie auch für Auslagerungen im Inland gelten, insbesondere die vertragliche Absicherung der datenschutzrechtlichen Betroffenenrechte, das Weisungsrecht des öffentlichen Organs, die Übernahme von datenschutzrechtlichen Pflichten durch die Empfängerin sowie die Wahrnehmung der Aufsicht durch die zuständige Datenschutzbehörde. Weitere

Informationen zu den unabhängig vom Angemessenheitsbeschluss geltenden Rahmenbedingungen bei der Auslagerung unter Beizug einer Cloud-Lösung enthält das Merkblatt Cloud-spezifische Risiken und Massnahmen.[7]

Bei der vertraglichen Absicherung der Betroffenenrechte ist darauf zu achten, dass der Aufwand, diese Rechte wahrzunehmen, in etwa dem Aufwand für eine Geltendmachung im Inland entspricht. Dasselbe gilt für die Durchsetzung von vertraglichen Rechten des öffentlichen Organs, die zur Wahrung von Betroffenenrechten notwendig sind. Aus diesem Grund sind für grenzüberschreitende Auslagerungen der Bearbeitung von Personendaten durch öffentliche Organe in der Regel die Wahl des schweizerischen Rechts sowie eines Gerichtsstands in der Schweiz erforderlich, um die Anforderungen an die Verhältnismässigkeit der Datenbearbeitung zu erfüllen.

Entscheidend für die Wirksamkeit des Swiss-U.S. DPF ist das institutionelle Umfeld zu deren Durchsetzung. Ohne wirksame Durchsetzungsmechanismen ist das DPF nicht in der Lage, die erhoffte Risikosenkung für Auftragsbearbeitungen in den USA zu bewirken. Entsprechend ist darauf zu achten, dass die Bedingungen der Auslagerung über den gesamten Zeitraum der geplanten Auslagerung stabil bleiben. Dies bedeutet, dass sowohl die Zertifizierung der Auftragnehmerin als auch die datenschutzrechtlichen Vereinbarungen sowie die Wirksamkeit des zu ihrer Durchsetzung notwendigen institutionellen Umfelds für die Dauer der Auslagerung gesichert sein müssen. Aus diesen Gründen muss ein Ausstiegsszenario erarbeitet werden, das gegebenenfalls eine datenschutzkonforme Fortführung der Datenbearbeitung ermöglicht.

In diesem Zusammenhang ist die Pressemitteilung vom 27. Januar 2025 des Privacy and Civil Liberties Oversight Board von Bedeutung, wonach der Präsident drei der insgesamt vier Mitglieder des Privacy and Civil Liberties Oversight Board entlassen habe, darunter auch den Chair.[8] Damit kann das Board das Quorum von drei Mitgliedern für gewisse Entscheidungen nicht erreichen. Im Rahmen des DPF hat das PCLOB eine Mitsprache bei der Wahl der Richterinnen und Richter des Data Protection Review Court sowie die Aufsicht über die Einhaltung des EO 14086 durch die Geheimdienste. Ein erster Bericht wurde für 2025 in Aussicht gestellt.[9]

4 Fazit

Mit Blick auf das volatile institutionelle Umfeld des DPF sowie die aktuellen Sparmassnahmen der U.S. Regierung erscheint unklar, für wie lange die Grundlagen des bundesrätlichen Angemessenheitsentscheids ihre Gültigkeit behalten werden.[10] Es ist daher angezeigt, zum

---

7 Abrufbar unter https://www.privatim.ch/de/uberarbeitetes-privatim-merkblatt-cloud-spezifische-risiken-und-massnahmen-2/ (Stand 16. April 2025).

8 https://documents.pclob.gov/prod/Documents/EventsAndPress/994df0d6-6bae-4284-a95f-3f3699e0a0f0/PCLOB%20press%20release%20(1-27-25)%20-%20508%20Complete.pdf

9 https://documents.pclob.gov/prod/Documents/EventsAndPress/6e6c7a7b-6036-4d6d-b635-ffb53f68e4f4/Statement%20on%20PCLOB%20Review%20Under%20Section%203%20of%20EO%2014086,%20Completed%20508,%20Nov%207%202024.pdf

10 In einem Interview vom 13. März 2025 betonte der zuständige EU Kommissar Micheal McGrath, dass die EU am DPF festhalte, die Kommission aber die Entwicklung in den USA bezüglich der Durchsetzungsmechanismen genau beobachte; siehe https://www.csis.org/analysis/future-transatlantic-digital-collaboration-eu-commissioner-michael-mcgrath (Stand 24. April 2025).

Zeitpunkt einer geplanten Übermittlung von Personendaten an eine private Organisation in den USA die Rechtslage im Bereich des Swiss-US DPF zu verifizieren.

Um auf künftige Änderungen reagieren zu können, sollten Prozesse, die eine Auslagerung der Bearbeitung von Personendaten an eine nach Swiss-U.S. DPF zertifizierte Organisation vorsehen, auf eine Art und Weise gestaltet werden, die es erlaubt, bei signifikanter Verminderung des datenschutzrechtlichen Schutzniveaus wirksame Massnahmen zum Schutz der Betroffenen zu ergreifen und/oder die entsprechenden Datenbearbeitungen in ein Land mit einem angemessenen Datenschutzniveau zu verlagern. Ein realistisches Ausstiegsszenario, das bei Bedarf umgesetzt werden kann, ist unabdingbar. Zu achten ist insbesondere auf Änderungen in den folgenden Bereichen:

- der Widerruf oder die Nichterneuerung des Zertifikats durch die Datenempfängerin;
- die Änderung bzw. Aufhebungen von einschlägigen Rechtsgrundlagen im US-amerikanischen Recht;
- die Wirksamkeit des zweistufigen Beschwerdeverfahrens;
- die Handlungsfähigkeit der Aufsichtsbehörden.

In diesem Zusammenhang ist darauf hinzuweisen, dass der Bundesrat im Rahmen der fortlaufenden Überprüfung der Voraussetzungen i.S.v. Art. 16 Abs. 1 DSG i. V. m. Art. 8 DSV berechtigt ist, den Angemessenheitsbeschluss gegebenenfalls zu widerrufen.

Aus diesen Gründen ist es erforderlich, die Datenschutz-Folgenabschätzungen in Zusammenhang mit Auslagerungen von Datenbearbeitungen in das US-amerikanische Ausland regelmässig zu überprüfen. Zu achten ist hierbei auf Änderungen in den materiellen und institutionellen Grundlagen, auf die sich der Angemessenheitsbeschluss des Bundesrates stützt, Änderungen in deren Anwendung durch US-Behörden und/oder in der entsprechenden Gerichtspraxis sowie Massnahmen der US-Regierung, welche die Finanzierung oder die Wirksamkeit der Beschwerde- und/oder Aufsichtsinstanzen beeinträchtigen. Entsprechend sind die folgenden, in der Änderungsverfügung des Bundesrates vom 14. August 2024 genannten Rechtsgrundlagen sowie die durch sie begründeten Institutionen anlassbezogen neu zu beurteilen:

- Swiss-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce;[11]
- Durchführungsverordnung (Executive Order des Präsidenten der USA; EO) 14086 vom 7. Oktober 2022;[12]
- Vorschrift über das Gericht zur Datenschutzüberprüfung des Generalstaatsanwalts der Vereinigten Staaten vom 7. Oktober 2022;[13]
- Richtlinie 126 der Nachrichtendienstgemeinschaft zur EO 14086;[14]

---

11 Abrufbar unter https://www.dataprivacyframework.gov/EU-US-Framework => Switzerland, (Stand 3. März 2025).

12 Abrufbar unter https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelli-gence-activities (Stand 3. März 2025).

13 Abrufbar unter https://www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court (Stand 3. März 2025).

14 Abrufbar unter https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf (Stand 3. März 2025).

- Anerkennung der Schweiz als qualifizierten Staat im Hinblick auf die Berechtigung zum Rechtsbehelfsverfahren gemäss Abschnitt 3 der Executive Order 14086 durch den US-Generalstaatsanwalt vom 7. Juni 2024.[15]

15 Abrufbar unter https://www.justice.gov/opcl/media/1355326/dl?inline (Stand 3. März 2025).