Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Der Beauftragte

CH-3003 Bern, EDÖB

Einschreiben
Suva
Generalsekretariat
Fluhmattstrasse 1
Postfach
6002 Luzern

Ihr Zeichen:
Unser Zeichen:
Sachbearbeiter/in:
Bern, 13. Mai 2022

Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace «M365»

unter besonderer Berücksichtigung des von der Suva thematisierten Zugriffs von US-amerikanischen Behörden auf Personendaten, die das Unternehmen in eine von der Firma Microsoft betriebene Cloud auslagert

Mit Schreiben vom 10. Dezember 2021 stellte die Suva dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragen EDÖB eine mit *Risikobeurteilung Projekt Digital Workplace «M365»* betitelte Dokumentation[1] zu. In diesem Projekt geht es um die damals unmittelbar bevorgestandene Auslagerung von bis anhin «on premise» bearbeiteten Personendaten der Suva in ein vom US-amerikanischen Konzern Microsoft auf schweizerischem Territorium betriebenes Rechenzentrum[2].

Gemäss Begleitschreiben der Suva vom 10. Dezember 2021 seien von dieser Auslagerung alle Sparten der Suva, d.h. die Unfallversicherung, die Militärversicherung sowie die zwei Rehabilitationskliniken betroffen. Allerdings sei eine Auslagerung des Klinik-Informationssystems KIS zu Microsoft derzeit nicht geplant. Auch seien die Kernsysteme der Suva derzeit nicht davon betroffen.

Bei den von der Auslagerung in die Cloud betroffenen Daten gehe es einerseits um Inhaltsdaten – also diejenigen Daten, welche die Suva in der Cloud-Anwendung speichern und bearbeiten wird – und andererseits um Mitarbeitendendaten (z.B. Zugriffsberechtigungen, Zugriffslogs, Supportanfragen).[3] Als typische Beispiele für Inhaltsdaten erwähnt die Suva Geschäftskorrespondenz, Fallmanagement-Dokumentationen, Projektunterlagen, Videokonferenzen, Telefonate, Weiterbildungsinhalte, Termine sowie E-Mails.[4]

---

[1] Risikobeurteilung Projekt Digital Workplace «M365» vom 12. November 2021 inkl. Anhänge 1 bis 10 (nachfolgend «Risikobeurteilung»).

[2] Nachfolgend wird in diesem Zusammenhang die Bezeichnung «Cloud» verwendet.

[3] Risikobeurteilung Rz. 11.

[4] Anhang 1 zur Risikobeurteilung, S. 9.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Angesichts der weiten Verbreitung der Produkte und Leistungen von Microsoft in der Privatwirtschaft und den öffentlichen Verwaltungen der Schweiz ist das dem EDÖB zur Kenntnis gebrachte Auslagerungsprojekt für eine breite Öffentlichkeit von Interesse. Nach seiner ersten vorläufigen Antwort vom 20. Dezember 2021 sieht sich der Beauftragte nach dem Studium der umfangreichen Unterlagen veranlasst, in Anwendung von Art. 31 Abs. 1 Bst. b des Bundesgesetzes über den Datenschutz[5] zu der ihm unterbreiteten Risikobeurteilung und den dort aufgezeigten Massnahmen

summarisch Stellung zu nehmen:

I. Keine Vorlagepflicht

1. Die Suva ist in datenschutzrechtlicher Hinsicht ein Bundesorgan i.S.v. Art. 3 Bst. h DSG und hat gemäss Eintrag im DATAREG[6] einen Datenschutzberater bzw. eine Datenschutzberaterin eingesetzt. Aus den zugestellten Dokumenten geht hervor, dass die Risikobeurteilung unter Mitwirkung der Fachstelle Datenschutz[7] bzw. der internen Datenschutzberaterin[8] erstellt worden ist. Der Beauftragte geht davon aus, dass die Auslagerung der Datenschutzberaterin in Anwendung von Art. 20 Abs. 2 VDSG[9] gemeldet worden ist.

2. Nach Art. 23 des neuen DSG vom 25. September 2020[10], welches voraussichtlich am 1. September 2023 in Kraft treten wird, müssen dem EDÖB Datenschutz-Folgenabschätzungen (DSFA) vorgelegt werden, wenn der Verantwortliche aufgrund der DSFA zum Schluss kommt, dass die geplante Bearbeitung trotz der vorgesehenen Massnahmen ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hat (Abs. 1).

3. Aus der Risikobeurteilung geht hervor, dass die Suva die Zulässigkeit der geplanten Auslagerung nach Massgabe eines risikobasierten Ansatzes beurteilt hat, der sie zum Ergebnis geführt hat, dass diese keine hohen Risiken für ihre Versicherten, die Patienten ihrer Kliniken sowie ihre Mitarbeitenden und sonstigen betroffenen Personen mit sich bringe[11]. Aufgrund dieses Beurteilungsergebnisses hätte somit auch bei einer Geltung des neuen Rechts keine Vorlagepflicht gegenüber dem EDÖB bestanden.

4. Nachdem der EDÖB von bestehenden Bearbeitungen oder digitalen Projekten von Bundesorganen Kenntnis genommen hat, kann er – unabhängig davon, ob eine Notwendigkeit zur Erstellung einer DSFA und eine Pflicht zur Vorlage derselben i.S.v. Art. 23 nDSG besteht – nach Art. 31 Abs. 1 Bst. b zu den datenschutzerheblichen Massnahmen Stel-

---

[5] Bundesgesetz über den Datenschutz (DSG; SR 235.1). Soweit die Suva Datenbearbeitungen, die Gegenstand des Projektes bilden, als private Person vornehmen sollte, stützt sich die vorliegende Stellungnahme auf Art. 28 DSG.

[6] Register der Datensammlungen nach Art. 28 VDSG.

[7] Risikobeurteilung Rz. 22.

[8] Anhang 5 zur Risikobeurteilung Rz. 2.

[9] Verordnung zum Bundesgesetz über den Datenschutz (VDSG); SR 235.11.

[10] Nachfolgend als «nDSG» bezeichnet.

[11] Risikobeurteilung Rz. 39.

lung nehmen, die das Bundesorgan trifft oder zu treffen beabsichtigt[12]. Vorbehalten bleibt jederzeit auch eine aufsichtsrechtliche Erhebung der relevanten Sachverhalte.

II. Dokumentation der Suva

5. In sachverhältlicher Hinsicht hat die Suva die Zielsetzungen, die nach betrieblichen Kriterien vorgenommene Auswahl der technischen Lösung und die Abwicklung ihres Auslagerungsprojekts dargelegt und dokumentiert.

6. Weiter hat die Suva die aus ihrer Sicht mit dem Übergang von der heutigen zur neuen Lösung einhergehenden Risiken für die Persönlichkeit der betroffenen Personen und die Massnahmen, die sie zu deren Minderung getroffenen hat, dokumentiert. Sie hat in ihrer Darstellung bei der Frage von Zugriffen durch ausländische Behörden einen Schwerpunkt gesetzt.

7. Die Suva hat auch dargelegt, dass ein erheblicher technologischer und finanzieller Druck bestehe, die fragliche Auslagerung rasch an die Hand zu nehmen. Trotzdem habe sie dafür gesorgt, dass die Möglichkeit einer Rückführung der ausgelagerten Daten «on premise» gewahrt bleibe.

8. Weiter hat die Suva dargelegt, dass die von der Schweizerischen Informatikkonferenz bereits mit Microsoft verhandelten Verträge zum Einsatz kommen. Die Suva führe mit Microsoft das Gespräch für weitere Vertragsanpassungen. Insbesondere strebe die Suva eine Klarstellung im Vertrag an, wonach die dort definierten standardisierten Instruktionen an Microsoft nicht auch Instruktionen zur Bearbeitung von Personendaten zu eigenen Zwecken von Microsoft beinhalten[13]. Die einschlägigen Bestimmungen der standardmässigen Verträge zur Auftragsbearbeitung verschaffen Microsoft namentlich die Möglichkeit, Personendaten des Kunden für eigene Zwecke zu bearbeiten.

III. Sicherheitstechnische Risiken

9. Auf eine umfassende Analyse der informationstechnischen Aspekte der Risikobeurteilung wird im Rahmen dieser summarischen Stellungnahme verzichtet. Dennoch weist der Beauftragte die Suva darauf hin, dass gewisse Risiken nur partiell identifiziert und bewertet worden sind. Insbesondere bezieht sich die Analyse gemäss DSFA[14] nur auf Risiken aufgrund der Auslagerung in die Cloud, nicht aber auf solche, die sich aus der Anwendung von Microsoft 365 an sich ergeben.

---

[12] Die wörtlich identische Bestimmung findet sich in Art. 58 Abs. 1 Bst. e nDSG.

[13] Vgl. Schreiben Suva an EDÖB vom 9. Februar 2022 Ziff. 4 c) sowie Anhang 9 der Risikobeurteilung Rz. 36.

[14] Anhang 8 zur Risikobeurteilung.

10. Ferner ist bekannt, dass gewisse Dienste in Microsoft 365 nicht end-to-end verschlüsselt sind (z.B. Microsoft Teams). Dem EDÖB sind Publikationen bekannt, in denen das Risiko beim Einsatz dieser Dienste als «hoch» bezeichnet worden ist[15]. Aus der Risikobeurteilung der Suva geht nicht hervor, wie sie diesen Aspekt einschätzt.

IV. Grenzüberschreitende Datenbekanntgabe in die USA

1. Suva thematisiert Problematik des fremden Behördenzugriffs

11. Die Suva geht davon aus, dass sich mit der Auslagerung eines Teils der Personendatenbearbeitung in eine vom US-amerikanischen Konzern Microsoft auf schweizerischem Territorium betriebene Cloud die Frage möglicher Zugriffe von US-amerikanischen Behörden auf die ausgelagerten Daten stellt.

12. Die Suva geht damit sinngemäss davon aus, dass mit der beschlossenen Auslagerung ein Datenexport in die USA einhergehen könnte.

2. EDÖB qualifiziert Auslagerung als grenzüberschreitende Datenbekanntgabe

13. Da die Suva ihre Vertragspartei verpflichtet hat, die ausgelagerten Daten in der Schweiz zu bearbeiten, geht es vorliegend nicht um die Frage eines möglichen Zugriffs fremder Behörden auf Personendaten, die unter Zustimmung der Bearbeitungsverantwortlichen von der Schweiz ins Ausland exportiert werden. Bei der von der Suva thematisierten Frage eines Zugriffs von US Behörden geht es vielmehr um einen von der Bearbeitungsverantwortlichen missbilligten Datenexport ins Ausland, der dadurch zustande kommen könnte, dass fremde Behörden auf ihre Vertragspartei Einfluss nehmen.

14. Nach Auffassung des EDÖB stellen sowohl der vom Bearbeitungsverantwortlichen gewollte, als auch der von ihm missbilligte Export von Personendaten eine «grenzüberschreitende Bekanntgabe» i.S.v. der Datenschutzgesetzgebung dar, weshalb die Bestimmungen von Art. 6 ff. DSG resp. Art. 16 ff. nDSG auf entsprechende Sachverhalte und somit auch die von der Suva beschlossene Auslagerung von Personendaten in eine vom US Konzern Microsoft in der Schweiz betriebene Cloud Anwendung finden.

3. Vorgaben des EDÖB zur grenzüberschreitenden Datenbekanntgabe in die USA

15. In der Schweiz waren die USA bis im Sommer 2020 auf der Staatenliste als Staat mit einem angemessenen Datenschutzniveau aufgrund des Swiss-USA Privacy Shields aufgeführt und ein Datenexport war unter Einhaltung von gewissen Vorgaben möglich. Der EDÖB entschloss sich im Spätsommer 2020 die Datenschutzkonformität des Privacy Shield Regimes neu zu evaluieren. Er fällte diesen Entschluss vor dem Hintergrund seiner jährlichen Überprüfungen des Swiss-US Privacy Shield Regimes und mit Blick auf die ergangene Rechtsprechung des Europäischen Gerichtshofs (EuGH) in Sachen Schrems II.

---

[15] vgl. "Public DPIA Teams OneDrive SharePoint and Azure AD" des Ministry of Justice and Security, Strategic Vendor Management Microsoft, Google and AWS (SLM Rijk) and SURF (IT procurement for Dutch universities) vom 16. Februar 2022 (https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad).

16. Das erwähnte Urteil des EuGHs ist in der Schweiz nicht anwendbar, und es gibt in der Schweiz auch keine entsprechende Judikatur. Angesichts dieser Ausgangslage sah sich der EDÖB mit Rücksicht auf das allgemeine Prinzip der Rechtsstaatlichkeit und das Bedürfnis nach Rechtssicherheit sowie seiner Aufgabe zur Führung der erwähnten Staatenliste und das Bedürfnis nach Rechtssicherheit veranlasst, eine Prüfung nach schweizerischem Recht vorzunehmen. Er kam dabei zum Schluss, dass die Platzierung der USA auf der von ihm publizierten Staatenliste nicht aufrechtzuerhalten war (vgl. Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG[16]). Aufgrund dieser Einschätzung hat der EDÖB in der erwähnten Staatenliste den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen.

17. Am 25. März 2022 hat die Europäische Kommission angekündigt, mit den USA Verhandlungen über eine Nachfolgereglung zum aufgekündigten Rahmenwerk Privacy Shield aufzunehmen. Der Beauftragte geht davon aus, dass der Bundesrat im Falle eines Zustandekommens einer neuen Vereinbarung zwischen der EU und den USA mit hoher Wahrscheinlichkeit eine analoge Neuregelung zwischen der Schweiz und den USA anstreben wird.

18. In casu ist der US Konzern Microsoft und die dazugehörenden Unternehmenseinheiten in der ganzen Welt und somit auch in der Schweiz dem US-Cloud Act[17] unterstellt. Dieser verpflichtet alle Unternehmenseinheiten, Zugriffe auf Personendaten durch US-Behörden auch dann zu gewährleisten, wenn die Datenspeicherung nicht in den USA erfolgt. Das Vorgehen nach Cloud Act erfolgt ohne Beachtung der von der schweizerischen Rechtsordnung verlangten Verfahren und Garantien. Zudem versetzen die USA ihre Sicherheitsbehörden und Nachrichtendienste rechtlich[18] und faktisch in die Lage, die auf US-Territorium ansässigen Mutterkonzerne dazu anzuhalten, ihren Geschäftsstellen im Ausland Aufträge zur Beschaffung von Personendaten ausländischer Staatsbürger zu erteilen.

19. Der EDÖB hat im Juni 2021 eine Anleitung[19] für das Verfahren für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug veröffentlicht. In dieser Anleitung wird das Vorgehen für die Prüfung der rechtlichen Zulässigkeit detailliert beschrieben.

---

[16] Öffentliche Stellungnahme des EDÖB vom 08.09.2020: https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html.

[17] Die USA haben den Clarifying Lawful Overseas Use of Data Act oder kurz Cloud Act im März 2018 verabschiedet. Er soll den US-Strafverfolgungsbehörden im Bereich der Verhütung, Ermittlung, Aufklärung oder Verfolgung schwerer Straftaten (serious crimes) den Zugriff auf Daten ermöglichen, die von Anbietern von Kommunikationsdiensten (Communication Service Providers, CSP) mit Sitz in den USA gespeichert worden sind. Dies unabhängig davon, ob die entsprechenden Daten in den USA oder, etwa über Tochtergesellschaften, im Ausland gespeichert sind.

[18] Gestützt auf Section 702 des Foreign Intelligence Surveillance Act (FISA) können Anbieter elektronischer Kommunikationsdienste verpflichtet werden, Daten an US-Geheimdienste weiterzugeben bzw. ihnen Zugang dazu zu gewähren.

[19] Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG), veröffentlicht im Juni 2021, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html, sowie als Beilage zu vorliegendem Schreiben.

20. In der vorgelegten Dokumentation geht die Suva auf das vom EDÖB für alle Datenexporte und somit auch für missbilligte und potentielle Exporte empfohlene Prüfverfahren nicht ein.

4. Risikobasierter Ansatz der Suva

21. Obwohl die Suva davon ausgeht, dass mit der beschlossenen Auslagerung ein Datenexport in die USA einhergehen kann, welche ein Land ohne angemessenes Datenschutzniveau sind, finden sich in ihren Ausführungen keine konkreten Aussagen zur datenschutzrechtlichen Zulässigkeit der Auslagerung resp. des damit verbundenen potentiellen Exports.

22. Die Suva bringt durch Benennung der von ihr eingereichten Dokumentation als «Risikobeurteilung» sinngemäss zum Ausdruck, dass die vorausgesehene Möglichkeit eines Zugriffs durch US Behörden auf die ausgelagerten Personendaten, der rechtlichen Zulässigkeit ihres Vorgehens nicht grundsätzlich entgegenstehe, sondern rechtlich zulässig sei, solange die von ihr geschätzte oder berechnete Wahrscheinlichkeit eines Datenzugriffs durch US Behörden einen von ihr als vertretbar erachteten Wert nicht überschreitet.

23. Im Rahmen ihres risikobasierten Ansatzes hält die Suva fest, dass sich die mit der Datenauslagerung einhergehende Möglichkeit eines justizförmigen, d.h. auf Rechtshilfeersuchen oder den US-Cloud Act gestützten, behördlichen Zugriffs auf die ausgelagerten Personendaten für den Betrachtungszeitraum von 5 Jahren «auf 2.52 % belaufe und damit höchst unwahrscheinlich sei»[20]. Bei diesem Wert, so die Suva, «komme es mit einer Wahrscheinlichkeit von 90 % statistisch gesehen (bei gleichbleibender Wahrscheinlichkeit) alle 903 Jahre mindestens ein Mal zu einem erfolgreichen Lawful Access»[21]. Auch unter Einschluss nicht justizförmiger Zugriffe durch US Nachrichtendienste schätzt die Suva die von ihr als «Risiko» bezeichnete Wahrscheinlichkeit insgesamt als «höchst unwahrscheinlich» ein, obwohl sie einräumt, dass «eine Unsicherheit bestehen bleibe»[22]. Zur Begründung führt sie namentlich an, dass die in die Cloud ausgelagerten Daten kaum Inhalte umfassten, die typischerweise Gegenstand von nachrichtendienstlichen Suchaufträgen aus diesem Land seien.

24. Die Suva berief sich bei der Darlegung ihres risikobasierten Ansatzes und den darauf gestützten Berechnungen auf eine von David Rosenthal entwickelte und publizierte Methode[23].

5. Vorbehalte des EDÖB gegen den risikobasierten Ansatz

25. Aus den Unterlagen der Suva geht eine Vielzahl von Annahmen hervor, die aufgrund der erwähnten Methode zur Berechnung der als «Risiko» bezeichneten Wahrscheinlichkeit behördlicher Zugriffe getroffen worden sind. Es fällt auf, dass diese Annahmen teilweise

---

[20] Risikobeurteilung Rz. 22.

[21] FN 12 zu Risikobeurteilung Rz. 22.

[22] Risikobeurteilung Rz. 41.

[23] David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020.

auf dem inhaltlichen Interessenwert beruhen, welchen die ausgelagerten Personendaten nach der Einschätzung der Suva für US-amerikanische Behörden haben könnten.

26. Die Bestimmungen zur Bekanntgabe von Personendaten ins Ausland unterscheiden nach dem geltenden wie auch dem neuen DSG[24] zwischen fremden Rechtsordnungen, die einen angemessenen Datenschutz gewährleisten, und solchen, welche dies nicht tun[25]. Die Anforderungen für Datenübermittlungen in Staaten ohne angemessenen Datenschutz sind im Gesetz aufgezählt. Hinweise auf Rechtfertigungsgründe oder Auslegungsargumente, die sich auf eine Differenzierung der nachrichtendienstlichen Interessenlage einzelner Exportstaaten und unternehmens- oder organspezifischen Inhalte der übermittelten Daten abstützen liessen, finden sich dort indessen nicht. Ebensowenig enthält der Gesetzeswortlaut Hinweise auf einen risikobasierten Ansatz zur Gewährleistung eines angemessenen Schutzes[26]. Daraus lässt sich nach Auffassung des EDÖB zwar nicht ableiten, dass risikobasierte Argumente im Sinne einer Ergänzung des von ihm empfohlenen Prüfverfahrens von Gesetzes wegen zwingend ausgeschlossen wären. Ergänzende Argumente dürfen jedoch nicht dazu führen, dass die im behördlichen Kontext grundrechtlich verbürgten Garantien aufgeweicht werden.

27. Vor diesem Hintergrund erscheint für den Beauftragten zumindest fraglich, ob der risikobasierte Ansatz rechtlich zulässig ist und angerufen werden darf, um die hier zur Diskussion stehenden Datenauslagerung zu rechtfertigen.

28. Zu dieser Frage existiert in der Schweiz zurzeit keine Rechtsprechung, weshalb sie der EDÖB auch mit Blick auf die vorerwähnte Möglichkeit einer Nachfolgereglung zum aufgekündigten Rahmenwerk Privacy Shield zurzeit offenlässt.

6. Risikobasierte Einzelargumente der SUVA

a) Organspezifische Inhalte der ausgelagerten Daten

29. Ausgehend von ihrer Tätigkeit als Versicherungsanstalt und den organspezifischen Inhalten des ausgelagerten Teils der Personendaten schätzt die Suva im Rahmen ihres risikobasierten Ansatzes die Wahrscheinlichkeit von Untersuchungen und Informationsbeschaffungen, welche sich direkt gegen die Suva als Datenherrin richten, als äusserst gering ein: nämlich auf einen Fall pro zehn Jahren[27].

30. Aufgrund der Einschätzung, wonach die Daten kaum Inhalte umfassen, die typischerweise Gegenstand von Suchaufträgen der US Nachrichtendienste seien, weist die Risikobeurteilung der Suva auch die Gefahr eines auf nachrichtendienstliche Anordnung hin verdeckt erfolgenden Datenabflusses durch den US-Mutterkonzern resp. die unter dessen Einfluss stehenden Unternehmenseinheiten in Europa und der Schweiz als äusserst gering aus. Ihre Risikobeurteilung geht davon aus, dass höchstens die Personendaten zur Militärversicherung von Interesse sein könnten[28].

---

[24] S. dazu vorne.

[25] Art. 6 DSG bzw. Art. 16 nDSG.

[26] Anders z.B. Art. 7 und 8 nDSG, die ausdrücklich einen risikobasierten Ansatz enthalten.

[27] Risikobeurteilung eines Lawful Access durch ausländische Behörden Ziff. 2 a) (Anhang 7 zur Risikobeurteilung).

[28] Risikobeurteilung eines Lawful Access durch ausländische Behörden Ziff. 4 d) (ebd.).

b) Vorbehalte des EDÖB

31. Neben den USA gibt es weitere, nach globalem Einfluss strebende Staaten, welche Drittstaatenangehörigen zurzeit keine mit der schweizerischen Datenschutzgesetzgebung vergleichbaren, gerichtlich einklagbaren Rechte zum Schutz ihrer Persönlichkeit einräumen und demzufolge nicht auf der Staatenliste des EDÖB aufgeführt sind. Es ist bekannt, dass die Sicherheitsbehörden und Nachrichtendienste solcher Staaten flächendeckende Recherchen über ihre Zielpersonen anzustellen pflegen. Sie verfügen über rechtliche Befugnisse und tatsächliche Möglichkeiten, die auf ihrem Territorium ansässigen Mutterkonzerne dazu zu veranlassen, Cloud-Daten sämtlicher Geschäftskunden nach Hinweisen auf Zielpersonen zu durchsuchen, die es den Diensten ermöglichen, ein möglichst umfassendes, lückenloses und intimes Bild ihrer Zielpersonen zu erlangen. Es muss mit anderen Worten damit gerechnet werden, dass die Nachrichtendienste von Mächten, die Drittstaatenangehörigen keinen hinreichenden Datenschutz gewährleisten, grundsätzlich alle Arten von Informationen akkumulieren, ohne dass dies für die Betroffenen erkennbar würde oder dass ihnen dagegen ein mit dem schweizerischen Recht vergleichbarer Rechtsschutz gewährt würde. Es muss weiter damit gerechnet werden, dass die Nachrichtendienste dieser Staaten insbesondere den Grundätzen der Zweckbindung und Verhältnismässigkeit geringe Bedeutung einräumen und von ihren Zielpersonen regelmässig auch private und intime Informationen wie Gesundheitsdaten beschaffen. Vor diesem Hintergrund stiesse die Annahme der Suva, wonach die ausgelagerten Daten kaum Inhalte umfassen, die typischerweise Gegenstand von nachrichtendienstlichen Suchaufträgen sein könnten, selbst bei einer Bejahung der Zulässigkeit ihres risikobasierten Ansatzes auf Bedenken.

32. Nach Auffassung des Beauftragten sollten Bundesorgane, die Teil eines engeren oder erweiterten Kreises der öffentlichen Verwaltung des Bundes sind, vor der Auslagerung von Personendaten berücksichtigen, dass die nachrichtendienstliche Datenbeschaffung fremder Staaten ohne angemessene Datenschutzgesetzgebung in der Regel gegen ausländische Gemeinwesen als Ganzes abzielt. Die Behörden solcher Staaten können zur Erreichung ihrer Beschaffungsziele hohen Druck auf die auf ihrem Territorium ansässigen Mutterkonzerne ausüben. Letztere wiederum können sich so veranlasst sehen, ihre Tochtergesellschaften und übrigen Geschäftsstellen in Europa und der Schweiz dazu anzuhalten, in den Personendatenbeständen mehrerer oder gar aller Geschäftskunden Suchaufträge auszuführen.

33. Somit erscheint fraglich, ob der organisationsspezifische Inhalt der Personendaten, die ein einzelnes Bundesamt oder ein einzelner Bundesbetrieb wie die Suva in einer Cloud von Microsoft bearbeiten lässt, im Rahmen ihres risikobasierten Ansatzes ein geeignetes Kriterium darstellen kann, um die Wahrscheinlichkeit eines Datenzugriffes durch fremde Behörden zu beurteilen. Aber auch, wenn man die Geeignetheit des Kriteriums bejahen wollte, erwiese sich die darauf gestützte tiefe Bewertung dieser Wahrscheinlichkeit durch die Suva, die als Bundesorgan zum erweiterten Kreis des Gemeinwesens der Eidgenossenschaft gehört, in dem von ihr vorgenommenen Umfang als unzureichend begründet.

c) Gesetzestreue des Schweizer Personals

34. In Anhang 9 der Risikobeurteilung wird aufgezeigt, dass ein allfälliger, auf das Mutterhaus in den USA ausgeübter Druck zur Herausgabe von Informationen seitens des für Microsoft tätigen Personals in Europa – und mit Blick auf das strafrechtliche Verbot, hoheitliche

Handlungen fremder Staaten zu unterstützten[29], auch in der Schweiz – auf Hindernisse treffen dürfte[30].

d) Vorbehalt des EDÖB

35. Der Beauftragte gibt zu bedenken, dass die behördlichen Zugriffe auch unter Anwendung technischer Massnahmen gelingen können, die dem in der Schweiz beschäftigten Personal verborgen bleiben.

7. Zusammenfassende Bemerkungen des EDÖB zur Angemessenheit der risikobasierten Einzelargumente der Suva

36. Insgesamt müsste sich die Zulässigkeit der Auslagerung und der damit einhergehenden Möglichkeit einer Datenbekanntgabe in die USA als Staat ohne angemessenes Datenschutzniveau selbst bei einer Bejahung der rechtlichen Zulässigkeit des risikobasierten Ansatzes der Suva als problematisch erweisen. Zum einen nahm sie diese Bewertung unter Anwendung von organspezifischen Kriterien vor, deren Geeignetheit zweifelhaft erscheint. Hinzu kommt, dass die Suva die Wahrscheinlichkeit eines Zugriffs durch US Behörden in ihrer Schätzung auf einen vernachlässigbar tiefen Wert gesenkt hat, dessen Herleitung aus Sicht des EDÖB in tatsächlicher Hinsicht unzureichend begründet bleibt.

37. Die Suva hat die Wahrscheinlichkeit eines Zugriffs durch eine Fremdbehörde nicht nur tief ausgewiesen, sondern aufgrund der angewandten Berechnungsmethode mit einer bis auf Hundertstel von Prozenten resp. mit auf Hunderte von Jahren extrapolierten Wahrscheinlichkeiten beziffert. Dieser Anspruch auf Wertgenauigkeit weckt Zweifel, steht er doch in einem offensichtlichen Kontrast zu den weiten Ermessensbandbreiten, die das Berechnungsmodell den Bearbeitungsverantwortlichen für die Annahmen einräumt, aus denen sich das bezifferte Risiko ableitet.

V. Verantwortlichkeit der Suva

38. Der EDÖB begrüsst, dass die Suva ihr Auslagerungsprojekts einer eigenverantwortlichen Datenschutz-Überprüfung unterzogen hat.

39. Der Beauftragte macht die Suva darauf aufmerksam, dass sie auf die Begründung der rechtlichen Zulässigkeit ihres Vorgehens nach Massgabe des von ihm empfohlen Prüfmodells verzichtet hat und ihr Vorgehen nach Massgabe eines risikobasierten Ansatzes rechtfertigt, der in der Datenschutzgesetzgebung des Bundes nicht vorgesehen ist.

40. Bei Festhalten an ihrem risikobasierten Ansatz rät der EDÖB der Suva, die mit der Auslagerung eines Teils ihrer Personendaten einhergehenden Risiken zeitnah einer Neubeurteilung zu unterziehen[31] sowie ihre Projektentscheide an die ihr zugänglichen Erkenntnisse über die relevante Sach- und Rechtslage anzupassen. Dazu gehört nach Auffassung des EDÖB die Berücksichtigung der richtungsweisenden Entscheide im Rahmen der

---

[29] Art. 271 StGB.

[30] a.a.O. Ziff. 36 Bst. d) und e).

[31] Gemäss Risikobeurteilung Rz. 5 sollte die vorliegende Risikobeurteilung einen Zeitraum von 5 Jahren ab 1. Januar 2022 abdecken und danach wiederholt werden.

Cloud-Strategie des Bundes[32] sowie der vorerwähnten Verhandlungen zu einer Nachfolgeregelung zum aufgekündigten Rahmenwerk Privacy Shield.

41. Der EDÖB hat von den Bemühungen der Suva um datenschutzrechtlich gebotene Zusatzvereinbarungen mit Microsoft und vom Umstand Kenntnis genommen, dass die Suva auf die datenschutzrechtlich angezeigte Klarstellung im Vertrag hinwirkt, dass die dort definierten standardisierten Instruktionen an Microsoft nicht auch Instruktionen zur Bearbeitung von Personendaten zu eigenen Zwecken von Microsoft beinhalten.

VI. Zusammenfassende Stellungnahme des EDÖB

1. Der Beauftragte hat von der Auslagerung eines Teils der von der Suva bearbeiteten Personendaten und den ihm freiwillig eingereichten Dokumenten sowie den dort aufgezeigten Massnahmen Kenntnis genommen und vorstehend dazu in Anwendung von Art. 31 Abs. 1 Bst. b DSG summarisch Stellung genommen.

2. Der EDÖB sieht zurzeit keine Veranlassung, den ihm zur Kenntnis gebrachten Sachverhalt von Amtes wegen zu untersuchen. Je nach Entwicklung der sachverhältlichen Situation und Rechtslage behält er sich jedoch vor, in einem späteren Zeitpunkt aufsichtsrechtlich tätig zu werden.

3. Der Beauftragte behält sich vor, seine Stellungnahme in Anwendung von Art. 30 Abs. 2 DSG nach deren Zustellung an die SUVA zu veröffentlichen.

4. Die Suva wird aufgefordert, den Beauftragten **bis am 30. Mai 2022** auf redaktionelle Fehler hinzuweisen und ihn auf gesetzlich geschützte Geheimnisse sowie Personendaten aufmerksam zu machen, die ihrer Ansicht nach von einer Publikation auszunehmen sind.

A. Lobsiger

Adrian Lobsiger

Beilage: Anleitung für das Verfahren für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug vom Juni 2021

[32] So gilt im Hinblick auf die noch ausstehenden rechtlichen, organisatorischen und technischen Abklärungen für die Bundesverwaltung, dass im Testbetrieb «CEBA Agil» für Microsoft 365 keine besonders schützenswerten Personendaten, keine vertraulichen Dokumente und keine Daten, welche dem Amtsgeheimnis unterliegen, gespeichert werden dürfen. Vgl. «Bund verlängert Testbetrieb von Microsoft 365» Medienmitteilung der Bundeskanzlei vom 22.02.2022 (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87286.html).

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 6 Abs. 2 lit. a DSG)

(veröffentlicht Juni 2021)

1. Zweck der Anleitung

Die vorliegende Anleitung soll Datenbearbeitern die Prüfung der Zulässigkeit von Datenübermittlungen von personenbezogenen Daten ins Ausland erleichtern.

Anhand eines Schemas erläutert diese Anleitung den Anwendungsfall des Datentransfers ins Ausland nach Art. 6 Abs. 2 lit. a DSG, wenn dort eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, und dieser Mangel durch hinreichende Garantien kompensiert werden muss (vgl. auch Art. 6 Abs. 2 und 3 der Verordnung zum Bundesgesetz über den Datenschutz VDSG, SR. 235.11). Auf die Voraussetzungen nach lit. b – g wird in dieser Anleitung nicht eingegangen.

SR 235.1 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)

Art. 6 Grenzüberschreitende Bekanntgabe

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

[2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten.

SR 235.11 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG)

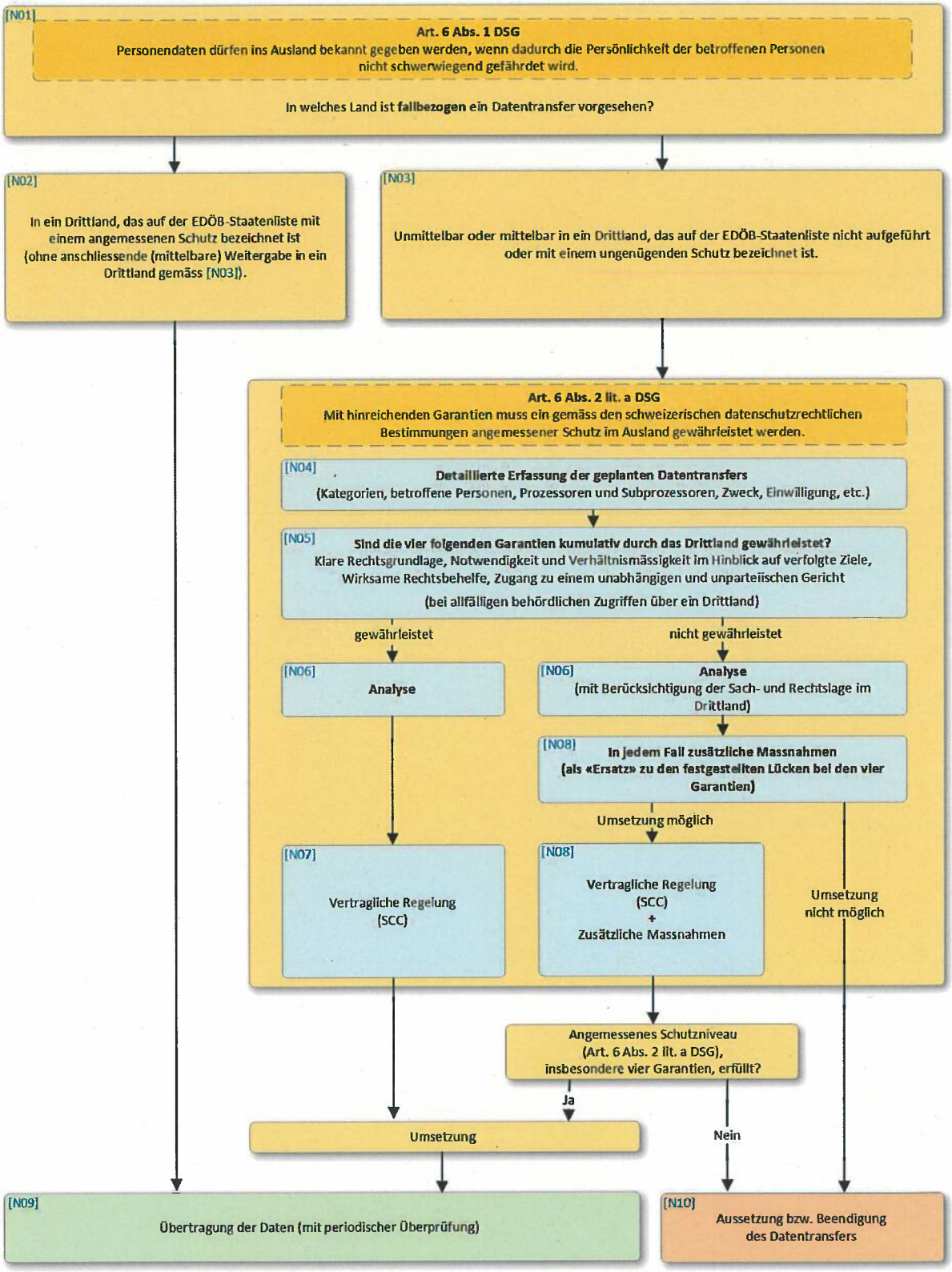
Art. 6 Informationspflicht

[2] Wurde der Beauftragte über die Garantien und die Datenschutzregeln informiert, so gilt die Informationspflicht für alle weiteren Bekanntgaben als erfüllt, die:

a. unter denselben Garantien erfolgen, soweit die Kategorien der Empfänger, der Zweck der Bearbeitung und die Datenkategorien im Wesentlichen unverändert bleiben; oder
b. innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfinden, soweit die Datenschutzregeln weiterhin einen angemessenen Schutz gewährleisten.

[3] Die Informationspflicht gilt ebenfalls als erfüllt, wenn Daten gestützt auf Musterverträge oder Standardvertragsklauseln übermittelt werden, die vom Beauftragten erstellt oder anerkannt wurden, und der Beauftragte vom Inhaber der Datensammlung in allgemeiner Form über die Verwendung dieser Musterverträge oder Standardvertragsklauseln informiert wurde. Der Beauftragte veröffentlicht eine Liste der von ihm erstellten oder anerkannten Musterverträge und Standardvertragsklauseln.

2. Ablaufschema



3. Erläuterungen

[N01] Überprüfung des Datenschutzniveaus im Drittland

Der verantwortliche Datenexporteur muss sicherstellen, dass bei der Bearbeitung der Daten in den Zielländern ein angemessenes Datenschutzniveau gewährleistet ist (Art. 6 DSG). Wenn die Daten in ein EU/EWR Land transferiert werden, kann von einem angemessenen Datenschutzniveau ausgegangen werden, wenn ein Weiterexport in ein Drittland ausgeschlossen ist.

Es ist zu beachten, dass ein Auftragsdatenbearbeiter bzw. –prozessor in einem Land mit angemessenem Datenschutzniveau unter Umständen einem Gesetz oder anderen zwingenden Vorgaben eines Drittlandes unterstehen kann, das diesen zur Bekanntgabe der Daten an die Behörden eines Drittlandes verpflichtet und diese Bekanntgaben z.B. intransparent oder nicht justiziabel sind (vgl. dazu im Einzelnen die Garantien in N05). In diesem Fall ist nach N03 zu verfahren (Bsp.: Server in der Schweiz, EU oder dem EWR eines Unternehmens, welches direkt oder indirekt einer staatlichen Rechtsordnung eines Staates ohne angemessenem Datenschutzniveau untersteht).

[N02] Angemessenheit (Art. 6 Abs. 1 DSG)

Exportstaat figuriert auf der EDÖB Staatenliste

Wenn der Inhaber von Datensammlungen Daten in einen Staat übermittelt, der auf der Staatenliste des EDÖB als ein solcher mit angemessenem Datenschutzniveau aufgeführt wird, gilt er als gutgläubig gemäss Art. 3 Abs. 1 ZGB. Allerdings handelt es sich um eine widerlegbare Vermutung. Der Inhaber der Datensammlung kann sich dann nicht auf seinen guten Glauben berufen, wenn er z.B. Kenntnis hat, dass in seinem spezifischen Fall das angemessene Datenschutzniveau in einem bestimmten Land dennoch nicht gewährleistet ist (Art. 3 Abs. 2 ZGB).

Der Datenexporteuer bleibt in jedem Fall für den Datenexport verantwortlich und muss sich periodisch darüber informieren, ob die Angemessenheit nach wie vor gilt und dass nicht andere Gründe (z.B. aufgrund von Hinweisen aus der Praxis oder den Medien) gegen eine sichere Bearbeitung der Personendaten im entsprechenden Zielland sprechen.

Exportstaat figuriert nicht auf der EDÖB Staatenliste

Figuriert ein Staat nicht auf der Staatenliste des EDÖB, bedeutet dies nicht automatisch, dass er keinen angemessenen Schutz gewährleistet. Der EDÖB hat nicht jeden Staat auf die Angemessenheit geprüft. Zudem kann nur ein schweizerisches Gericht verbindlich und abschliessend über die Anwendung von Art. 6 DSG entscheiden. Der Datenexporteur muss deshalb in diesem Fall die nötigen Rechtsabklärungen selbst vornehmen, z.B. durch Konsultation von Lehre und Rechtsprechung oder das Einholen von unabhängigen Rechtsgutachten.

[N03] Kein angemessener Schutz gemäss der Staatenliste des EDÖB oder Anzeichen, dass keine datenschutzkonforme Datenübertragung möglich ist (Art. 6 Abs. 2 lit. a DSG)

Fehlt der Staat als angemessen auf der Staatenliste des EDÖB oder bestehen trotz Vorhandenseins auf der Staatenliste konkrete Hinweise, wonach mit Blick auf den beabsichtigten Export nicht von einem angemessenen Datenschutzniveau ausgegangen werden kann, muss der Datenexporteur den Datenschutz mit hinreichenden Garantien, insbesondere durch einen Vertrag, sicherstellen. Grundlage werden in der Regel **Mustervertragsklauseln, sog. Standard Contract Clauses (SCC)** sein. Anzumerken ist, dass unternehmensinterne Datenschutzvorschriften, sog. **Binding Corporate Rules (BCR),** welche die Datenbekanntgabe ins Ausland innerhalb eines Konzerns oder zwischen verschiedenen Unternehmen unter einheitlicher Leitung regeln, von einem Datenexporteur im externen Verhältnis nicht als Ersatz von SCC verwendet werden können. BCRs sind ohne Zustimmung des externen Datenexporteurs und unabhängig von der Vertragslaufzeit meistens vom Datenimporteur individuell abänderbar und es fehlen zudem wesentliche Bestandteile, die in einem SCC abgebildet sind (z.B. Bestimmungen betreffend die Einsetzung von Subunternehmern).

[N04] Detaillierte Erfassung des Datentransfers

Eine detaillierte Erfassung des Datentransfers durch den Datenexporteur, z.B. mittels eines Verzeichnisses, ist die sachdienliche Basis für die Einschätzung des beabsichtigten Datenexports.

Es ist unter anderem Folgendes zu klären:

- Weisen die zu exportierenden Daten einen Personenbezug auf?
- Sind Personen bestimmt oder bestimmbar?
- Was ist der Zweck der Datenbekanntgabe?
- Welche Kategorien von Personendaten werden übermittelt?
- Gibt es weitere Auftrags- und Unterauftragsbearbeiter und befinden sich diese in Drittländern?
- Werden die Personendaten von Unternehmen bearbeitet, welche Rechtsordnungen in Drittländern unterstehen (z.B. US-amerikanische Cloudanbieter mit Servern in CH/EU/EWR)?
- Werden die Daten innerhalb des Drittlandes oder in ein weiteres Drittland weiterübermittelt oder gibt es Hinweise, dass es dazu kommen könnte?

[N05] Vier Garantien

Mit Blick auf behördliche Zugriffe im Drittland (z.B. zwecks nationaler Sicherheit oder Strafverfolgung) und die Rechte der Betroffenen hat der Datenexporteur zu prüfen, ob jene mit dem schweizerischen Datenschutzrecht und den schweizerischen Verfassungsgrundsätzen vereinbar sind. Er muss entsprechende Abklärungen selbst vornehmen und darf sich dabei nicht nur auf die Aussagen des Datenimporteurs verlassen. Dies kann er durch Konsultation von Literatur und Rechtsprechung oder das Einholen von unabhängigen Rechtsgutachten machen.

Folgende schweizerische Grundrechtsgarantien müssen im Drittland analog gewährleistet sein und es gilt zu prüfen, welche Mängel im Drittland vorliegen:

1. **Legalitätsprinzip: Klare, präzise und zugängliche Regeln (Art. 5 und Art. 164 BV)**
   Hinreichend bestimmte und klare Rechtsgrundlage betreffend Zwecke sowie Verfahren und materiellrechtliche Voraussetzungen des behördlichen Datenzugriffs und Befugnisse der Behörden.

2. **Verhältnismässigkeit der Befugnisse und Massnahmen im Hinblick auf die verfolgten Regelungsziele (Art. 5 Abs. 2 BV und Art. 4 Abs. 2 DSG)**
   Die Befugnisse und Massnahmen der Behörden müssen geeignet und erforderlich sein, um die gesetzlichen Zwecke der behördlichen Zugriffe zu erfüllen. Zudem müssen sie für die Betroffenen zumutbar sein.

3. **Dem Einzelnen müssen wirksame Rechtsmittel zur Verfügung stehen (Art. 13 Abs. 2 BV zur Durchsetzung von Art. 15 DSG sowie Art. 8 EMRK)**
   Betroffene in der Schweiz müssen wirksame gesetzlich verankerte Rechtsbehelfe für die Durchsetzung ihrer Rechte zum Schutz der Privatsphäre und informationellen Selbstbestimmung (z.B. Auskunft-, Berichtigungs- und Löschungsrecht) haben.

4. **Rechtsweggarantie und Zugang zu einem unabhängigen und unparteiischen Gericht (Art. 29 ff. BV und Art. 15 DSG)**
   Eingriffe in die Privatsphäre und informationelle Selbstbestimmung müssen einem wirksamen, unabhängigen und unparteiischen Kontrollsystem unterliegen (Gericht oder andere unabhängige Stelle, z. B. Verwaltungsbehörde oder parlamentarisches Gremium). Neben vorheriger (gerichtlichen) Genehmigung von Überwachungsmassnahmen (Schutz vor Willkür) muss auch die tatsächliche Funktionsweise des Überwachungssystems überprüft werden können.

Hinweis Anwendungsfall USA

Bestehen Anhaltspunkte, dass Personendaten in den USA direkt oder indirekt bearbeitet werden bzw. bearbeitet werden könnten, insbesondere bei Nutzung von Clouddiensten, kann der Fragebogen im Anhang für weitere Abklärungen verwendet werden [«*Datenschutzanfrage an Dienstleister/Anbieter mit möglichen direkten oder indirekten US-Beziehungen (mit Einbezug deren Subunternehmer unter weiteren Sub-Sub-Unternehmer und weiteren Dienstleistern/Anbietern)*»].

[N06] Analyse

Es ist eine Analyse des Datentransfers im Einzelfall und in Bezug auf das gewählte Instrument wie SCC sowie die rechtlichen Umstände im Drittland vorzunehmen. Der verantwortliche Datenexporteur muss bei der Erfassung und Analyse des Datentransfers alle nötigen Abklärungen vornehmen (z.B. Einholen von unabhängigen Rechtsgutachten).

In die Prüfung ist u.a. Folgendes miteinzubeziehen:

- Geltende Rechtsvorschriften im Zielland
- Praxis der Verwaltungsbehörden und Gerichtsbehörden
- Rechtsprechung

[N07] Garantien gewährleistet: SCC

Wenn die vier Garantien (vgl. N05) gewährleistet sind, kann mit standardmässigen SCC ein angemessenes Datenschutzniveau erreicht werden.

Es bleibt dann lediglich noch bei der individuellen Umsetzung der SCC zu berücksichtigen, ob sich eventuell weitere vertragliche Massnahmen zum individuellen Schutz (nicht gegen staatliche Zugriffe) aufdrängen. Solche Regelungen können z.B. folgende Bereiche miteinbeziehen:

- Betroffenenrechte stärken (z.B. Auskunftsrecht)
- Regelung von technischen Massnahmen als Bedingung für Datenübermittlungen vorsehen
- Befugnis des Datenexporteurs stärken, indem der Datenimporteur verpflichtet wird, sich bei den Datenbearbeitungssystemen Inspektionen zu unterziehen und Rechenschaft abzulegen
- Klauseln vorsehen, die bei Bedarf schnelles Verfahren der Datensicherung ermöglichen.

[N08] Garantien nicht gewährleistet: SCC und zwingend zusätzliche Massnahmen

Wenn die in N05 erwähnten Garantien im Drittland nicht umfassend gewährleistet sind, sind vorab in jedem Fall zusätzliche Massnahmen zu prüfen, die als „Ersatz" für die fehlenden vier Garantien dienen.

Zusätzliche vertragliche Massnahmen (zwischen dem Datenexporteur und dem Datenimporteur) sind kaum möglich, weil sie drittstaatliche Behörden nicht binden können und dadurch behördliche Zugriffe nicht verhindern können. Beispielsweise sind auch Schadenersatzregelungen, die Zusicherung der Ergreifung von Rechtsbehelfen und Ausschöpfung von Rechtsmitteln gegen behördliche Anordnungen oder Transparenzberichte sind insbesondere dann ungenügend, wenn rechtliche Vorgaben im Drittstaat vorgehen bzw. diese vertraglichen Massnahmen durchkreuzen.

Die **zusätzlichen technischen und organisatorischen Massnahmen** müssen dergestalt sein, dass die Behördenzugriffe auf die übermittelten Personendaten im Zielland faktisch verhindert werden. Bei der Datenhaltung im Sinne eines reinen Cloud-Betriebs durch Dienstleister eines Staates ohne angemessenes Schutzniveau wäre z.B. eine Verschlüsselung denkbar, welche nach den Prinzipien BYOK («bring your own key») und zusätzlich BYOE («bring your own encryption») umgesetzt ist, so dass in der Cloud keine Klardaten vorliegen resp. in der Cloud keine Entschlüsselung und Verschlüsselung erfolgt. Bei über die reine Datenhaltung hinausgehenden Dienstleistungen im Zielland gestaltet sich der Einsatz solcher technischen Massnahmen indessen als anspruchsvoll.

Ergibt die Prüfung, dass das Fehlen einer oder mehrerer der vier Garantien gemäss N05 nicht durch zusätzliche Massnahmen ausgleichbar ist, muss nach N10 verfahren werden.

[N09] Übertragung der Daten

Nach Umsetzung der nötigen zusätzlichen Massnahmen muss der verantwortliche Datenexporteur regelmässig die sachlichen und rechtlichen Voraussetzungen überprüfen. Kommt er zum Schluss, dass die Datenschutzkonformität nicht mehr gegeben ist, ist nach N10 zu verfahren.

[N10] Aussetzung bzw. Beendigung der Datenbekanntgabe ins Ausland

Wenn mit zusätzlichen Massnahmen die festgestellten Mängel bezüglich der Erfüllung der vier Garantien nicht kompensiert werden können und damit keine hinreichende Garantie nach Art. 6 Abs. 2 lit. a DSG erreicht wird, ist der Datentransfer ins Ausland umgehend auszusetzen bzw. zu beendigen.

Anhang[1]

Datenschutzanfrage an Dienstleister/Anbieter mit möglichen direkten oder indirekten US-Beziehungen (mit Einbezug deren Subunternehmer unter weiteren Sub-Sub-unternehmer und weiteren Dienstleistern/Anbietern)

Dienstleister/Anbieter inkl. alle nachfolgenden Subunternehmer und beigezogene Dienstleister/Anbieter (auch von Software-Komponenten) nachfolgend «SIE»

Angesichts des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18, insbesondere jedoch nicht abschliessend der Absätze 138 bis 145, bitten wir dringend um Klärung der folgenden Fragen:

1 Direkte Anwendung von 50 U.S.C. § 1881a (= FISA 702)

1.1 Fallen SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten, die an SIE übermittelt werden, verarbeitet oder Zugang zu diesen Daten hat, unter eine der folgenden Definitionen in 50 U.S.C. § 1881(b)(4), die SIE oder die andere(n) Stelle(n) direkt unter 50 U.S.C. § 1881a (= FISA 702) fallen lassen könnte(n)?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

1.2 Insbesondere,

A. Sind SIE oder eine andere relevante US-Einheit ein Telekommunikationsunternehmen, wie dieser Begriff in Abschnitt 153 von Titel 47 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

B. Sind SIE oder eine andere relevante US-Einheit ein Anbieter von elektronischen Kommunikationsdiensten, wie dieser Begriff in Abschnitt 2510 von Titel 18 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

C. Sind SIE oder eine andere relevante US-Einheit ein Anbieter eines Ferncomputerdienstes, wie dieser Begriff in Abschnitt 2711 von Titel 18 U.S.C. definiert ist?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

[1] Der vorliegende Fragebogen wurde auf der Grundlage des Fragebogens von www.noyb.eu an die Schweiz angepasst und weiterentwickelt.

D. Sind SIE oder eine andere relevante US-Einheit ein anderer Anbieter von Kommunikationsdiensten, der Zugang zu drahtgebundener oder elektronischer Kommunikation hat, entweder wenn diese Kommunikation übertragen wird oder wenn diese Kommunikation gespeichert wird?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

E. Sind SIE oder eine andere relevante US-Einheit ein leitender Angestellter, Angestellter oder Vertreter einer Einheit, die unter die obigen Buchstaben (A), (B), (C), oder (D) fällt?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

2.1 Werden SIE von einer US-Muttergesellschaft oder einem US-Aktionär kontrolliert, oder haben SIE eine andere relevante Verbindung zu den USA, die das US-Recht indirekt gegen SIE durchsetzbar machen könnte?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

2.2 Wenn ja, sind SIE nach EU-Recht, nationalem Recht, Gesellschaftsrecht und internationalem Privatrecht verpflichtet, Anordnungen, Ersuchen oder Direktiven von US-Einrichtungen zu ignorieren, die von Ihnen verlangen würden, personenbezogene Daten, die SIE verarbeiten, der US-Regierung gemäss 50 U.S.C. § 1881a (= FISA 702) oder EO 12.333 offenzulegen, und sind SIE in der Lage, einen solchen Zugriff faktisch zu sperren?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

Bitte geben SIE an, auf welche rechtlichen und/oder technischen Schutzmassnahmen SIE sich berufen:

3 Verarbeitung unter EO 12.333

Arbeiten SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten verarbeitet, die von uns an SIE übermittelt werden, in irgendeiner Hinsicht mit den US-Behörden zusammen, die die Überwachung der Kommunikation gemäss EO 12.333 durchführen, sollte dies obligatorisch oder freiwillig sein?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

4 Andere anwendbare Gesetze

Unterliegen SIE oder eine andere relevante US-Einheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die personenbezogene Daten verarbeitet, die von uns an SIE übermittelt werden, einem anderen Gesetz, das als Beeinträchtigung des Schutzes personenbezogener Daten nach der DSGVO (Artikel 44 DSGVO) oder von schweizerischem Recht angesehen werden könnte?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

wenn ja, geben SIE bitte diese Gesetze an:

5 Massnahmen gegen massenhafte und unterschiedslose Verarbeitung im Transitverkehr (FISA 702 und EO 12.333)

Weil auch der Gerichtshof im obengenannten Urteil die Notwendigkeit betont hat, sicherzustellen, dass personenbezogene Daten im Transit nicht der Massenüberwachung unterliegen, bitten wir um folgende Klarstellungen:

A. Haben SIE geeignete technische und organisatorische Massnahmen (siehe Artikel 32 DSGVO) für jeden Schritt der Verarbeitungsvorgänge getroffen, die sicherstellen, dass eine massenhafte und unterschiedslose Verarbeitung personenbezogener Daten durch oder im Auftrag von Behörden im Transitverkehr (z.B. im Rahmen des "Upstream"-Programms in den USA) unmöglich gemacht wird?

☐ Ja ☐ Nein ☐ Wir sind gesetzlich verpflichtet, diese Frage nicht zu beantworten

B. Wenn ja, geben SIE bitte an, welche technischen und organisatorischen Massnahmen (einschliesslich Verschlüsselung) getroffen wurden, damit weder Inhalts- noch Metadaten von hochentwickelten staatlichen Akteuren mit direktem Zugang zum Internet-Backbone, zu Switches, Hubs, Kabeln und Ähnlichem verarbeitet werden können:

6 Beantwortung der oben gestellten Fragen

Wir bitten Sie, diese Fragen ohne unnötige Verzögerung zu beantworten, jedoch nicht später als fünf Arbeitstage ab Zugang dieses Fragebogens.

[Ort und Datum]

[Firma]

[rechtsgültige Unterzeichnung]