Blinde Passagiere

ESTA, CBP und die Daten derer, die nie gebucht haben.

Bettina Sterner, BA
kaffeekipferl.at
Mai 2026

Die in diesem Whitepaper enthaltenen Ausführungen, Analysen und Schlussfolgerungen spiegeln ausschließlich die persönliche fachliche Einschätzung der Autorin zum Zeitpunkt der Veröffentlichung wider. Sie sind unabhängig entstanden und stehen in keinem Zusammenhang mit aktuellen oder früheren Arbeitgebern, Auftraggebern, Mandanten oder sonstigen Organisationen, denen die Autorin angehört oder angehört hat. Das Whitepaper ersetzt keine rechtliche oder regulatorische Beratung im Einzelfall.

Abstract (Deutsch)

Seit Dezember 2025 plant die US-Behörde Customs and Border Protection (CBP) eine tiefgreifende Erweiterung des ESTA-Antragsverfahrens. Geplant sind unter anderem die Erhebung biometrischer Daten, Social-Media-Verläufe der letzten fünf Jahre, vollständige biographische Profile von Familienangehörigen sowie eine Umstellung auf mobile-only mit NFC-basierter Passchip-Auslesung und Echtzeit-Gesichtserkennung. Der EDPB hat im März 2026 förmlich interveniert und grundrechtliche Bedenken geäußert. Das vorliegende Whitepaper analysiert die datenschutzrechtlichen Konsequenzen für europäische Arbeitgeber, die Mitarbeiterinnen und Mitarbeiter in die USA entsenden. Im Mittelpunkt steht die These, dass der Arbeitgeber zwar nicht Verantwortlicher für die Verarbeitung durch CBP/DHS ist — wohl aber für die Entscheidung, die diese Verarbeitung unausweichlich macht. Aus dieser Rolle als strukturell Veranlassende/r ergeben sich Transparenzpflichten, eine Prüfpflicht zur Erforderlichkeit der Reise, die Notwendigkeit einer Datenschutz-Folgenabschätzung sowie technische und organisatorische Schutzmaßnahmen. Besondere Aufmerksamkeit gilt der Drittbetroffenheit von Familienangehörigen, die keine eigenständige Entscheidung getroffen haben und gegenüber DHS/CBP keinerlei durchsetzbare Betroffenenrechte besitzen. Für Unternehmen im DORA-/NIS2-Scope wird darüber hinaus auf die sicherheitsrechtliche Dimension von CBP-Gerätedurchsuchungen an der US-Grenze hingewiesen. Die DSGVO endet an der US-Grenze. Die datenschutzrechtliche Sorgfaltspflicht des Arbeitgebers tut es nicht.

Abstract (English)

Since December 2025, U.S. Customs and Border Protection (CBP) has been planning a significant expansion of the ESTA application process. Proposed changes include the collection of biometric data, five years of social media history, comprehensive biographical profiles of family members, and a shift to mobile-only processing with NFC-based passport chip reading and real-time facial recognition. In March 2026, the European Data Protection Board (EDPB) formally intervened, raising fundamental rights concerns. This whitepaper analyses the data protection implications for European employers who send employees on business trips to the United States. The central argument is that while employers are not controllers in respect of CBP/DHS processing, they are responsible for the decision that makes such processing unavoidable. This role as structural instigator gives rise to transparency obligations, a duty to assess whether the trip is genuinely necessary, a requirement to conduct a Data Protection Impact Assessment, and an obligation to implement appropriate technical and organisational safeguards. Particular attention is given to the position of family members — individuals who have made no independent decision and who hold no enforceable data subject rights against DHS/CBP. For organisations within the scope of DORA and NIS2, the paper also highlights the security-law dimension of CBP device searches at the U.S. border. The GDPR ends at the U.S. border. An employer's duty of care under data protection law does not.

Abgrenzung — Geltungsbereich: Datenschutzrechtliche Pflichten nach der DSGVO. Arbeitsrechtliche Fragestellungen bleiben weitgehend außer Betracht. **Ausnahme:** Eine freiwillige Betriebsvereinbarung nach österreichischem Recht wird berücksichtigt, soweit sie den betrieblichen Umgang mit Dienstreisen in die USA regelt.
Stand: Mai 2026; CBP-Vorschlag noch nicht in Kraft.

Hintergrund: CBP-Proposal & EDPB-Reaktion

> *Seit Dezember 2025 plant die US-Behörde Customs and Border Protection (CBP), eine nachgeordnete Behörde des Department of Homeland Security (DHS), eine tiefgreifende Erweiterung des ESTA-Antragsverfahrens[1]. Der EDPB hat im März 2026 förmlich interveniert — mit grundrechtlichen Bedenken, die für jeden europäischen Arbeitgeber mit Dienstreisen in die USA unmittelbar relevant sind.*

CBP-Notice vom 12. Oktober 2025

CBP schlug im Rahmen des Paperwork Reduction Act eine umfassende Revision der im ESTA-Verfahren erhobenen Datenfelder vor.[2] Die Kommentarfrist endete am 9. Februar 2026.[3] Zum Zeitpunkt dieser Analyse ist die Regelung noch nicht in Kraft.

Die geplanten Erweiterungen beruhen auf zwei präsidialen Rechtsinstrumenten: der Executive Order 14161 vom Januar 2025 (*Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats*) sowie dem Memorandum vom 4. April 2025 (*Updating All Forms to Collect Baseline Biographic Data*), das CBP angewiesen hat, auf sämtlichen Formularen sogenannte „high value data fields" zu erheben. Die Social-Media-Pflicht ist damit kein Gegenstand des laufenden Notice-and-Comment-Verfahrens, sondern präsidiales Sicherheitsmandat — sie wird unabhängig vom Ausgang der Kommentarphase umgesetzt werden.

Für ESTA umfassen die vorgesehenen Neuerungen: Social-Media-Verläufe der letzten fünf Jahre; Telefonnummern der letzten fünf Jahre; E-Mail-Adressen der letzten zehn Jahre; IP-Adressen und Metadaten aus elektronisch eingereichten Fotos; Biometrie (Gesicht, Fingerabdruck, DNA, Iris); Geschäftstelefonnummern (fünf Jahre) und Geschäfts-E-Mail-Adressen (zehn Jahre); ein vollständiges biographisches Profil der Familienangehörigen — Namen, Telefonnummern, Geburtsdaten, Geburtsorte und Wohnadressen von Eltern, Ehepartnern, Geschwistern und Kindern; sowie eine Umstellung auf Mobile-only.

Die Umstellung auf Mobile-only ist keine technische Nebensache. Die CBP-App ermöglicht die NFC-basierte Auslesung des ePassport-Chips — einschließlich kryptografischer Verifikation des Country Signing Certificate — sowie Liveness Detection und Facial Recognition über den CBP Traveler Verification Service (TVS). Ein Antrag über die Website kann diese Verifikationstiefe nicht erreichen**. Mobile-only bedeutet daher:** Jede*r ESTA-Antragsteller*in aus dem EWR wird künftig zwingend in ein biometrisches Echtzeit-Erfassungs- und Abgleichsystem eingebunden. Der TVS gleicht das eingereichte Gesichtsbild gegen einen bestehenden CBP-Biometriebestand ab — Umfang, Zusammensetzung und Retention dieses Bestands sind nicht öffentlich bekannt und werden im EDPB-Brief vom 10. März 2026 explizit als ungeklärte Frage benannt. Anträge, die die

1 ESTA (Electronic System for Travel Authorization) ist das US-amerikanische elektronische Reisegenehmigungssystem für Staatsangehörige aus Ländern des Visa Waiver Program (VWP), darunter alle EU-Mitgliedstaaten sowie Österreich. Die Genehmigung ist Voraussetzung für die visafreie Einreise in die USA für Aufenthalte bis zu 90 Tagen und muss vor Reiseantritt beantragt werden.

2 CBP, Notice of Proposed Information Collection — ESTA, Federal Register, 12. Oktober 2025. https://public-inspection.federalregister.gov/2025-22461.pdf

3 Paperwork Reduction Act, 44 U.S.C. § 3501 et seq.; Kommentarfrist endete am 9. Februar 2026.

kryptografische Validierung nicht bestehen, werden automatisch abgelehnt — ohne menschliche Prüfung.

Verfahrensrechtliche Anmerkung. *Die Änderungen wurden nicht als förmliches Rulemaking, sondern als „Information Collection Request" veröffentlicht. Das senkt die prozedurale Hürde erheblich — unabhängig von den eingereichten Kommentaren. Die auf EO 14161 gestützten Anforderungen sind davon unabhängig: Sie gelten kraft präsidialer Anordnung.*

Voluntary Self-Reported Exit (VSRE) Pilot und I-94-Automatisierung

CBP implementiert parallel eine neue Funktionalität innerhalb der CBP Home-App: Den Voluntary Self-Reported Exit (VSRE) Pilot. Reisende, die I-94-Anforderungen unterliegen, können bei der Ausreise aus den USA freiwillig biographische Passdaten, ein Gesichtsbild und Geolokationsdaten übermitteln — als Nachweis ihrer Ausreise. Die Nutzung ist optional; die Übermittlung eines Gesichtsbilds ist jedoch obligatorischer Bestandteil der Funktionalität. CBP verwendet Geolokationsdaten, um zu bestätigen, dass sich der/die Reisende tatsächlich außerhalb der USA befindet, sowie Liveness Detection, um die Echtheit des Selfies zu verifizieren. Das eingereichte Bild wird anschließend gegen bereits bei CBP gespeicherte Biometrie-Daten abgeglichen, um die Ausreise biometrisch zu bestätigen.

Datenschutzrechtlich ist die „optional but required"-Konstruktion heikel: Die Funktionalität ist freiwillig, ein Gesichtsbild einzureichen aber obligatorisch. In Kombination mit dem ESTA-Einreiseprozess vervollständigt CBP damit ein biometrisch bestätigtes Bewegungsprofil — Einreise, Aufenthalt via I-94, Ausreise — für EU-Reisende.

EDPB-Brief vom 10. März 2026

Der Europäische Datenschutzausschuss (European Data Protection Board / „EDPB") richtete am 10. März 2026 einen formellen Brief an Kommissar McGrath und Kommissar Brunner.[4] Der EDPB benennt vier Kernbedenken: Die Erhebung — insbesondere Social-Media-Verläufe und Daten unbeteiligter Familienangehöriger — ist in ihrer Notwendigkeit nicht begründet. Es ist unklar, ob EU-Bürgerinnen und -Bürger Betroffenenrechte gegenüber CBP überhaupt ausüben können. Zu Speicherdauer und Datanlöschung fehlen klare Regelungen. Und laufende Verhandlungen zu „Enhanced Border Security Partnerships" könnten Grundrechte zusätzlich beeinträchtigen.

Rechtlicher Status des EDPB-Briefes. *Der Brief richtet sich an die Europäische Kommission, nicht an CBP und nicht an einzelne Arbeitgeber. Er begründet keine unmittelbaren Rechtspflichten, ist aber ein klares Signal, dass die Aufsichtsbehörden die Situation als grundrechtlich problematisch bewerten.*

[4] EDPB, Brief an Kommissarin McGrath und Kommissar Brunner, 10. März 2026. https://www.edpb.europa.eu/system/files/2026-03/edpb_letter_20260310_us-legislative-developments_en.pdf

Datenschutzrechtliche Einordnung der erhobenen personenbezogenen Daten

Die geplanten Erweiterungen betreffen mehrere Datenkategorien, die datenschutzrechtlich unterschiedlich zu qualifizieren sind:

Datenkategorie	Einstufung	Besonderheit
Biographische Grunddaten	„Gewöhnliche" personenbezogene Daten	Bereits bisher erhoben; keine Änderung
NFC-Chipdaten (ePassport)	**Teils biometrische Daten, Art. 9 Abs. 1 DSGVO**	Auslesung über CBP-App; kryptografisch verifiziert gegen Country Signing Certificate; höhere Datenqualität als Webantragsstellung; Ablehnung bei fehlgeschlagener Validierung automatisch, ohne menschliche Prüfung
Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person (Gesicht, Fingerabdruck, Iris, DNA)	**Besondere Kategorie pb Daten, Art. 9 Abs 1 DSGVO**	Abgleich via CBP Traveler Verification Service (TVS) gegen bestehenden CBP-Biometriebestand; Umfang und Retention des Bestands ungeklärt
Social-Media-Verlauf (der jeweils letzten 5 Jahre)	Personenbezogene Daten; ggf. Art. 9 Abs 1 DSGVO relevant (polit. Meinung, Religion indirekt erkennbar, sexuelle Orientierung, gesundheitsbezogene Informationen)	Rückwirkend; kann unbeteiligte Dritte betreffen
Daten von Familienangehörigen (Eltern, Ehepartner*in, Geschwister, Kinder)	**Personenbezogene Daten Dritter**	**Vollständiges biographisches Profil: Namen, Telefonnummern (5 Jahre), Geburtsdaten, Geburtsorte, Wohnadressen; diese Personen haben die Daten nicht selbst übermittelt; keine Betroffenenrechte gegenüber DHS/CBP**
IP-Adresse, Geolokation und Gesichtsbild bei Ausreise (VSRE Pilot)	Biometrische Daten; Standortdaten	Formal freiwillig, Gesichtsbild aber obligatorischer Bestandteil; Abgleich gegen bestehenden CBP-Biometriebestand; vervollständigt biometrisch bestätigtes Bewegungsprofil
Geschäftskontaktdaten (Telefon 5 Jahre, Email 10 Jahre)	Personenbezogene Daten	Explizit getrennt von privaten Kontaktdaten erhoben; direkte Verbindungslinie zum Arbeitgeber für DHS/CBP sichtbar und dauerhaft erfasst; nachrichtendienstlich verwertbar

Kritischer Punkt: Daten von Familienangehörigen. *Die Erhebung betrifft Personen, die keine Entscheidung über die Dienstreise getroffen haben und gegenüber US-Recht vollständig schutzlos sind. Ein berechtigtes Interesse des Arbeitgebers nach Art. 6 Abs. 1 lit. f DSGVO ist zwar nicht von vornherein ausgeschlossen — die Entsendung des Mitarbeiters verfolgt einen legitimen Geschäftszweck. Die Abwägung dürfte jedoch schwer zugunsten des Arbeitgebers ausfallen: Die betroffenen Familienangehörigen haben keine Beziehung zum Arbeitgeber, keine vernünftigerweise zu erwartende Datenverarbeitung und keine durchsetzbaren Rechte gegenüber CBP.*

Verantwortlichenstruktur bei Dienstreisen in die USA

> *In der Reisekette agieren mehrere Akteur*innen als eigenständige oder veranlassende Verantwortliche. Der/die Arbeitgeber*in ist nicht Verantwortlicher für die Verarbeitung durch CBP — aber er/sie ist Verantwortlicher für die Entscheidung, die diese Verarbeitung erst notwendig macht.*

Akteur	DSGVO-Rolle	Eigene Verarbeitungen	Besonderheit
Arbeitgeber*in	Verantwortlicher (Art. 4 Nr. 7 DSGVO)	Buchungsdaten, Reisemanagement, HR	**Verantwortliche*r (Art. 4 Nr. 7 DSGVO) für die eigenen Reiseverarbeitungen (Buchung, HR, Dienstreiseentscheidung); bestimmt Zweck und Mittel der Entsendung und löst damit die ESTA-Pflicht unausweichlich aus. Die nachgelagerte Verarbeitung durch CBP ist unmittelbare und vorhersehbare Folge — begründet jedoch keine gemeinsame Verantwortlichkeit mit CBP.**
Arbeitnehmer*in	Betroffene*r; formal Antragsteller*in bei CBP	—	Faktisch ohne Wahl; Einwilligung strukturell unwirksam (Erwägungsgrund 43 DSGVO)
Airline	Eigenständige Verantwortliche	PNR, API an CBP	Kein Auftragsverarbeiter des Arbeitgebers; nicht kontrollierbar (EU-US PNR-Abkommen 2012)
CBP / DHS	US-Behörde; DSGVO nicht anwendbar	ESTA-Daten	Retention unklar; Betroffenenrechte für EU-Bürger*innen faktisch nicht ausübbar

Der/die Arbeitgeber*in als strukturell Veranlassende*r der Verarbeitung

Anm.: Diese Lesart des Verantwortlichkeitsbegriffs ist in der europäischen Aufsichtspraxis noch nicht förmlich verfestigt, folgt aber konsequent aus dem Zusammenspiel von Rechenschaftspflicht, Datenminimierung und dem Grundsatz der Zweckbindung.

Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO scheidet aus: CBP/DHS unterliegen nicht dem räumlichen Anwendungsbereich der DSGVO.[5]

Die eigentliche Frage lautet nicht, ob der/die Arbeitgeberin Verantwortlicher für die CBP-Verarbeitung ist — das scheidet aus. **Die Frage ist: Welche datenschutzrechtlichen Pflichten entstehen aus der Entscheidung, Mitarbeiter*innen in eine Situation zu schicken, in der eine umfangreiche Datenverarbeitung durch eine Drittstaatsbehörde unausweichlich wird?** Als Verantwortlicher für seine/ihre eigenen Verarbeitungen — Buchung, Reisemanagement, Dienstreiseweisung — trägt der/die

[5] Weil CBP/DHS US-Bundesbehörden sind, die auf US-Territorium im Rahmen des US-amerikanischen Rechts handeln: Die DSGVO gilt gemäß Art. 3 DSGVO für Verantwortliche, die in der EU niedergelassen sind, oder — über den Marktortgrundsatz — für Verantwortliche außerhalb der EU, die Waren oder Dienstleistungen an betroffene Personen in der EU richten oder deren Verhalten in der EU beobachten. Keine dieser Alternativen ist erfüllt: CBP/DHS richten ihre Tätigkeit nicht an Personen in der EU, sondern erfassen Personen, die in die USA einreisen wollen — der Verarbeitungsvorgang findet außerhalb der EU statt und zielt nicht auf den EU-Markt.

Arbeitgeber*in die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO für die vorhersehbaren Folgen dieser Entscheidungen.

Konsequenz. *Der/die Arbeitgeber*in ist nicht datenschutzrechtlich verantwortlich für das, was CBP mit den Daten tut. Er/sie ist jedoch verantwortlich für die Entscheidung, seine/ihre Mitarbeiter*innen in eine Situation zu schicken, in der diese Verarbeitung unausweichlich wird. Die damit verbundenen Pflichten sind nicht delegierbar.*

Sonderfall: Daten von Familienangehörigen

Der/die Arbeitgeber*in bestimmt über Zweck und Mittel der Reise und löst damit die ESTA-Pflicht unausweichlich aus. CBP erhebt auf Basis des Memorandums vom 4. April 2025 dabei auch ein vollständiges biographisches Profil der Familienangehörigen des/der Antragsteller*in: Namen, Telefonnummern der letzten fünf Jahre, Geburtsdaten, Geburtsorte und aktuelle Wohnadressen von Eltern, Ehepartner*innen, Geschwistern und Kindern. Diese Personen haben keine Beziehung zum/zur Arbeitgeber*in und haben keine Entscheidung über die Dienstreise getroffen. Ihre Daten werden vom/von der Antragsteller*in — faktisch ohne Alternative — an DHS/CBP übermittelt. Sie selbst haben auf diesen Vorgang keinen Einfluss und gegenüber DHS/CBP keinerlei durchsetzbare Betroffenenrechte. Ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO ist nicht von vornherein ausgeschlossen — die Entsendung verfolgt einen legitimen Geschäftszweck. Die Abwägung dürfte jedoch wie zuvor dargestellt nur schwerlich zugunsten des/der Arbeitgeber*in ausfallen.

Konsequenz für die Verhältnismäßigkeitsprüfung. *Die Drittbetroffenheit ist ein eigenständiges Argument für ein striktes Erforderlichkeitsgebot: Die Dienstreise muss nicht nur für den Geschäftszweck notwendig, sondern auch unter Berücksichtigung der Drittbetroffenheit verhältnismäßig sein.*

Einwilligung als Rechtsgrundlage — scheidet aus

Der Arbeitgeber kann das Risiko nicht durch eine Einwilligung des/der Arbeitnehmer*in abdelegieren. Einwilligung im Arbeitsverhältnis ist nur dort wirksam, wo die Verarbeitung im eindeutigen Interesse des/der Arbeitnehmer*in liegt — etwa bei freiwilligen Benefits oder der Anmeldung zur Betriebsveranstaltung.[6] Eine Dienstreise dient primär dem Geschäftszweck des/der Arbeitgeber*in; ein eindeutiger Benefit für den/die Arbeitnehmer*in, der die strukturelle Freiwilligkeitsproblematik überwinden könnte, ist im Regelfall nicht erkennbar.

Rechtsgrundlage für die veranlasste Verarbeitung

Der/die Arbeitgeber*in übermittelt selbst keine Daten an DHS/CBP — die Übermittlung erfolgt durch den/die Arbeitnehmer*in im Rahmen des ESTA-Antrags, der durch diese*n höchstpersönlich zu stellen ist.

Art. 6 Abs. 1 lit. b DSGVO — die Vertragserfüllung — scheidet als Rechtsgrundlage aus. Die Norm setzt voraus, dass die Verarbeitung erforderlich ist für die Erfüllung eines Vertrags, dessen Partei die betroffene Person ist. Dienstreisen mögen arbeitsvertraglich vereinbart sein; die Erhebung biometrischer Daten, von Social-Media-Verläufen und vollständiger biographischer Profile von Familienangehörigen ist jedoch keine notwendige Bedingung für die Erfüllung des Arbeitsvertrags. Das Erforderlichkeitskriterium ist eng auszulegen: Die Verarbeitung muss objektiv unerlässlich sein — nicht bloß nützlich oder aus Arbeitgeber*innensicht zweckmäßig. Maßgeblich ist dabei auch, ob weniger eingreifende Alternativen zur Erreichung desselben Ziels bestehen.[7] Wo Videokonferenz oder ein

[6] Erwägungsgrund 43 DSGVO; EDPB, Guidelines 05/2020 on consent, Rz 21 ff.

[7] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, Rz. 25.

Meetingort außerhalb der USA als realistische Option in Betracht kommt, fehlt es bereits an der Erforderlichkeit — unabhängig davon, ob die Reise geschäftlich sinnvoll wäre.

Der/die Arbeitgeber*in ist jedoch der-/diejenige, der/die die Situation schafft, in der diese Übermittlung unausweichlich wird. Als Rechtsgrundlage für diese Entscheidung kommt Art. 6 Abs. 1 lit. f DSGVO in Betracht — das berechtigte Interesse an der Durchführung der Geschäftsreise. Ob die Abwägung tatsächlich zugunsten des/der Arbeitgeber*in ausfällt, ist angesichts des Umfangs der erhobenen Daten, der fehlenden Betroffenenrechte gegenüber DHS/CBP und der ungeklärten Retention-Praxis jedoch alles andere als gesichert — und wird im Einzelfall von der tatsächlichen Erforderlichkeit der Reise und dem Fehlen zumutbarer Alternativen abhängen.

Die Konsequenz eines negativen Abwägungsergebnisses ist unmittelbar: Wenn die Interessen und Grundrechte der betroffenen Mitarbeiter*innen — und der betroffenen Familienangehörigen — überwiegen, entfällt die Rechtsgrundlage für die Dienstreiseweisung. Der/die Arbeitgeber*in darf die Reise in diesem Fall datenschutzrechtlich nicht anordnen. Die Frage, ob eine Dienstreise in die USA rechtmäßig ist, ist damit keine rein organisatorische Entscheidung mehr — sie ist eine datenschutzrechtliche Abwägungsentscheidung mit dokumentationspflichtiger Begründung.

Eine freiwillige Betriebsvereinbarung kann hier eine sinnvolle ergänzende Maßnahme sein: Sie schafft einen transparenten betrieblichen Rahmen, dokumentiert die Information der Arbeitnehmer*innen und kann — soweit der/die Arbeitgeber*in auf Einwilligung als ergänzende Grundlage setzen möchte — strukturell sicherstellen, dass diese Einwilligung tatsächlich freiwillig erfolgt. Das Problem der Familienangehörigen löst sie freilich nicht: Deren Daten werden übermittelt, ohne dass sie selbst Partei der Betriebsvereinbarung sind oder sein können.

Pflichten des/der Arbeitgeber*in aus der Rolle dessen, der/die die Dienstreise veranlasst

Transparenzpflicht

Die Informationspflicht des/der Arbeitgeber*in speist sich aus zwei Quellen. Für die eigenen Verarbeitungen im Reisekontext — Buchungsdaten, Reisegenehmigung, HR-Dokumentation — gilt Art. 13 DSGVO unmittelbar. Darüber hinaus ergibt sich aus dem Transparenzgrundsatz (Art. 5 Abs. 1 lit. a DSGVO) i.V.m. der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) eine weitergehende Pflicht zur aktiven Information: Der/die Arbeitgeber*in schafft durch die Dienstreiseentscheidung die Situation, in der die CBP-Verarbeitung unausweichlich wird — und muss Mitarbeiter*innen deshalb auch darüber informieren, welche Daten CBP erhebt, dass Familienangehörige betroffen sind und dass gegenüber DHS/CBP keine Betroffenenrechte ausübbar sind. Beide Pflichten können in einer einzigen integrierten Information erfüllt werden.

Diese Pflicht kann nicht mit dem Verweis auf das CBP-Portal erfüllt werden. Die interne Mitarbeiter*innen-Datenschutzerklärung sollte daher um einen Abschnitt zu Drittstaatsreisen ergänzt werden — mit Hinweis auf den fehlenden Angemessenheitsbeschluss[8], unklare Aufbewahrungs- und Löschfristen und dass betroffene Personen gegenüber DHS/CBP keine Betroffenenrechte haben.

[8] Das EU-US Data Privacy Framework (Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023, C(2023) 4745) gilt ausschließlich für die Übermittlung personenbezogener Daten an zertifizierte US-Unternehmen. US-Bundesbehörden wie DHS/CBP sind nicht zertifizierungsfähig und fallen nicht in den Anwendungsbereich des Frameworks. Eine auf den Angemessenheitsbeschluss gestützte Übermittlungsgrundlage scheidet daher aus. Auch Art. 49 DSGVO

Datenminimierungsprinzip (Art. 5 Abs. 1 lit. c DSGVO[9])

Die Entscheidung, eine*n Mitarbeiter*in in die USA zu entsenden, löst eine umfangreiche Datenverarbeitung aus. Der Grundsatz der Datenminimierung verlangt, dass der/die Arbeitgeber*in vorab prüft, ob die Reise tatsächlich erforderlich ist — oder ob Alternativen in Betracht kommen: Videokonferenz, lokale Partner*innen, Meetingort außerhalb der USA.

Besondere Sensibilität: Mitarbeiter*innen von Unternehmen im DORA-/NIS2-Scope. *CBP-Gerätedurchsuchungen an der US-Grenze sind nach US-Recht ohne Verdachtsmoment zulässig. Eine solche Durchsuchung kann je nach Einzelfall — insbesondere bei Zugang zu Unternehmensdaten oder privilegierten Systemen — einen sicherheitsrelevanten Vorgang darstellen, der auf seine Meldepflichtigkeit nach DORA bzw. NISG 2026 zu prüfen ist. Ob die einschlägigen Meldeschwellen erreicht sind, hängt vom Einzelfall ab: Maßgeblich sind insbesondere die Art der auf dem Gerät zugänglichen Systeme, der Umfang eines etwaigen Datenzugangs und die Klassifikation des/der betroffenen Mitarbeiter*in im internen Berechtigungskonzept. Für Mitarbeiter*innen mit privilegiertem Systemzugang besteht somit eine Schutzpflicht, die über datenschutzrechtliche Erwägungen hinausgeht.*

Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Der/die Arbeitgeber*in ist nach Art. 32 DSGVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko, das mit einer konkreten Verarbeitung personenbezogener Daten verbunden ist, angemessenes Schutzniveau zu gewährleisten. Bei Dienstreisen in die USA gehört dazu sicherlich die Bereitstellung gesonderter, minimal beladener Reisegeräte ohne dauerhaften Produktionssystemzugang — die Nutzung privater oder regulärer Dienstgeräte ist keine ausreichende Maßnahme. Darüber hinaus sind Verschlüsselung lokaler Daten und VPN-Verpflichtung zu implementieren sowie ein definiertes Verfahren für den Fall einer Gerätedurchsuchung festzulegen. Zu den organisatorischen Maßnahmen kann etwa auch die Bereitstellung eines rechtlichen Beistands zählen — etwa über eine Rechtsschutzversicherung mit Vor-Ort-Support —, der Mitarbeiter*innen im Fall einer Grenzkontrolle unmittelbar zur Verfügung steht.

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Der/die Arbeitgeber*in wird voraussichtlich für seine/ihre eigenen Verarbeitungen im Reisekontext eine Datenschutz-Folgenabschätzung durchführen müssen. Die Schwelle „voraussichtlich hohes Risiko" nach Art. 35 Abs. 1 DSGVO dürfte überschritten sein — nicht weil der/die Arbeitgeber*in selbst biometrische Daten verarbeitet oder die Drittstaatsübermittlung vornimmt, sondern weil seine/ihre eigene Verarbeitung (Reisegenehmigungsentscheidung, Buchung, HR-Dokumentation) eine Situation schafft, die für die betroffenen Arbeitnehmer*innen und ihre Familienangehörigen mit hohem Risiko verbunden ist: Die Datenverarbeitung durch CBP ist unausweichliche Folge dieser Entscheidung, die betroffenen Personen haben gegenüber DHS/CBP keinerlei durchsetzbare Rechte, Speicherdauer und Löschpraxis sind ungeklärt, und Familienangehörige sind betroffen, ohne selbst Entscheidungsträger*innen zu sein. Dieses aus der eigenen Verarbeitungsentscheidung resultierende Risiko für Rechte und Freiheiten natürlicher Personen trägt die DSFA-Pflicht.

Die DSFA hat die Erforderlichkeit der Reise, die Verhältnismäßigkeit der damit verbundenen Datenverarbeitung und die verfügbaren technischen und organisatorischen

(Ausnahmen für besondere Situationen) begründet keine geeignete Transfergrundlage für die vorliegende Konstellation: Die in Betracht kommenden Ausnahmen — insbesondere lit. d (wichtiges öffentliches Interesse) und lit. e (Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) — setzen eine spezifische Zweckbindung voraus, die bei der routinemäßigen ESTA-Verarbeitung im Rahmen von Dienstreisen nicht gegeben ist. Darüber hinaus gilt: Der/die Arbeitgeber*in übermittelt selbst keine Daten an DHS/CBP — die Übermittlung erfolgt durch den/die Arbeitnehmer*in. Eine Transferverantwortung des/der Arbeitgeber*in nach Art. 44 ff. DSGVO scheidet daher aus; die Frage einer geeigneten Transfergrundlage stellt sich für ihn/sie nicht unmittelbar.

[9] „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein."

Schutzmaßnahmen zu dokumentieren — und ist bei wesentlichen Änderungen der Sachlage zu aktualisieren.

Daten von Familienangehörigen — de facto keine datenschutzkonforme Lösung

Die Übermittlung von Daten der Familienangehörigen durch den/die Antragsteller*in ist unmittelbare Folge der Dienstreiseentscheidung. Eine Rechtsgrundlage nach Art. 6 Abs. 1 lit. f DSGVO ist zwar nicht von vornherein ausgeschlossen, die Abwägung dürfte jedoch schwerlich zugunsten des/der Arbeitgeber*in ausfallen — die betroffenen Personen haben keine Beziehung zum/zur Arbeitgeber*in, es ist keine vernünftigerweise zu erwartende Datenverarbeitung und zudem sind keine durchsetzbaren Rechte gegenüber DHS/CBP verbrieft. Der/die Arbeitgeber*in hat die Pflicht, Mitarbeiter*innen vorab zu informieren, damit diese ihrerseits ihre Familienangehörigen informieren können.

Fazit

Für Arbeitgeber*innen im EWR verschärft sich eine Pflichtenlage, die bereits bisher bestand. Die Entscheidung, Mitarbeiter*innen in die USA zu entsenden, verlangt eine aktive Prüfung der Erforderlichkeit, eine transparente Information der Betroffenen — einschließlich der Drittbetroffenheit von Familienangehörigen — eine Datenschutz-Folgenabschätzung sowie, bei Mitarbeiter*innen von Unternehmen im DORA-/NIS2-Scope, konkrete technische Schutzmaßnahmen. Ob die Abwägung nach Art. 6 Abs. 1 lit. f DSGVO im Einzelfall zugunsten des Arbeitgebers ausfällt, hängt maßgeblich davon ab, ob die Reise tatsächlich erforderlich ist und keine zumutbaren Alternativen bestehen.

Der/die Arbeitgeber*in ist nicht Verantwortlicher für das, was CBP mit den Daten tut — aber er/sie ist Verantwortlicher für die Entscheidung, seine/ihre Mitarbeiter*innen in eine Situation zu schicken, in der diese Verarbeitung unausweichlich wird. Die DSGVO endet an der US-Grenze. Die datenschutzrechtliche Sorgfaltspflicht des Arbeitgebers tut es nicht.
