

Übereinkommen zwischen den Parteien der Konvention über die polizeiliche Zusammenarbeit in Südosteuropa über den automatisierten Austausch von DNA-, daktyloskopischen- und Fahrzeugregisterdaten

Datenschutz-Folgenabschätzung gem. Art. 35 EU-Datenschutz-Grundverordnung

SYSTEMATISCHE BESCHREIBUNG

der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen

Art und Umfang der Verarbeitung (ErwG 90 DSGVO)

Entsprechend des Art. 27 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftätern oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (DSRL-PJ) idgF in Verbindung mit den Erläuternden Bemerkungen Nr. 94 der DSRL-PJ ist die Durchführung von Datenschutz-Folgenabschätzungen für die Prümer Kooperation und dortigen höchsten Datenschutzstandards explizit als nicht notwendig ausgeschlossen. Ungeachtet der bestehenden Prümer Zusammenarbeit, welche bereits seit 2006 zwischen Österreich und EU-Mitgliedstaaten sowie seit 2017 für die Prümer Zusammenarbeit im Bereich daktyloskopischer Daten etwa mit den Vereinigten Staaten von Amerika in Echtbetrieb steht, und keine neue Technologie darstellt sowie in über 16 Jahren verbindlichen Echtbetriebs zwischen allen EU-Mitgliedstaaten keine Risiken für persönliche Daten erkennen ließ, wird eine Datenschutz-Folgenabschätzung hiermit durchgeführt.

Der automatisierte Datenaustausch auf Grundlage des Übereinkommens stellt eine Erweiterung der bestehenden und auf EU Recht basierenden Prümer Zusammenarbeit dar. Dieser Datenaustausch zwischen Sicherheits- und Strafverfolgungsbehörden ist bereits im Unionsrecht datenschutzrechtlich sehr detailliert geregelt und wurde nun in das Übereinkommen übernommen. Sowohl EU-Mitgliedstaaten als auch EU-Beitrittskandidaten müssen vor deren EU-Beitritt einen solchen Datenaustausch rechtsverbindlich umsetzen.

Gemäß Art. 2 Abs. 1 des Übereinkommens richten die Vertragsparteien nationale DNA-Analysedateien für strafrechtliche Ermittlungen ein und leisten Unterstützung bei der Identifizierung von vermissten Personen und nichtidentifizierten sterblichen Überresten. Dazu gewähren die Vertragsparteien den nationalen Kontaktstellen anderer Vertragsparteien Zugriff zu Referenzdaten in ihren DNA-Analysedateien. Dieser Zugriff umfasst auch die Möglichkeit, eine automatisierte Suche durch Abgleich von DNA-Profilen durchzuführen (Art. 3).

Für die Datenübermittlung im Rahmen des Übereinkommens werden durch die von der Europäischen Kommission den Westbalkanstaaten eingeräumten Nutzungsmöglichkeiten verschlüsselte Datenkommunikationskanäle der Europäischen Union verwendet, welche grundsätzlich nur EU-Mitgliedstaaten und deren Organen und Behörden zugänglich sind. Es handelt sich bei dieser Kooperation um ein bewährtes EU Kooperationsmodell basierend auf anonymisierten Suchanfragemechanismen. Diese garantieren, dass es nur im Fall von mit forensischen Gutachten bestätigten Personenübereinstimmungen der biometrischen Daten zu einer Übermittlung von personenbezogenen Personaldaten zum Zweck der Bekämpfung internationaler Kriminalität und Terrorismus kommt.

Zwecke der Verarbeitung (Art. 35 Abs. 7 lit. a DSGVO):

Zweck dieses Übereinkommens ist die grenzüberschreitende polizeiliche Zusammenarbeit bei Bedrohung der öffentlichen Sicherheit im Hinblick auf die verstärkte Verhinderung, Verfolgung und Aufklärung von Straftätern, wie dies bereits in der Polizeikooperationskonvention für Südosteuropa (PCC SEE) festgelegt ist. Für diesen Zweck enthält das Übereinkommen Vorschriften für den automatisierten Austausch von DNA-Daten, daktyloskopische Daten und Fahrzeugregisterdaten sowie für den darauffolgenden Austausch von personen- und fallbezogenen Daten im Trefferfall.

Die Prümer Zusammenarbeit wird inhaltlich mit den selben Sicherheits- und Datenschutzstandards auf die Westbalkanstaaten erweitert. Die Westbalkanstaaten, die zwischenzeitlich alle EU Beitrittskandidatenstatus besitzen, haben die Prümer Kooperationsform vor EU Beitritt verbindlich gegenüber allen anderen EU-Mitgliedstaaten umzusetzen und anzuwenden.

BEWERTUNG

der Notwendigkeit und Verhältnismäßigkeit

Die im Übereinkommen enthaltenen Regelungen über den Austausch von personen- und fallbezogenen Daten im Trefferfall dienen einem der in Art. 8 Abs. 2 EMRK genannten Ziele, nämlich dem Schutz der nationalen Sicherheit sowie der öffentlichen Ruhe und Ordnung. Die Notwendigkeit ergibt sich aus dem wichtigen öffentlichen Interesse an der bestmöglichen Aufklärung schwerster Straftaten, der Ausforschung von Straftäterinnen und Straftätern sowie der Aufdeckung von Falschidentitäten.

RISIKEN (Art. 35 Abs. 7 lit. c DSGVO):

Durch die Einbeziehung der Westbalkanstaaten in die bestehende Prümer Zusammenarbeit wird einerseits der Adressatenkreis angepasst und andererseits ein Anstieg der Übermittlungen personenbezogener Daten ins Ausland und der Datenverarbeitungsvorgänge erfolgen. Zur Risikobewertung ist festzuhalten, dass nach über 16 Jahren Operativverfahren im Rahmen der Prümer Zusammenarbeit, in welchem bislang keine einzige Datenschutzverletzung oder fehlerhafte Datenverarbeitungen in einem EU-Mitgliedstaat bekannt wurde, der Datenaustausch ausreichend abgesichert ist und dass auch weiterhin keine Risiken zu erwarten sind, zumal identische Sicherheits- und Datenverarbeitungsprozesse im Rahmen der Prümer Zusammenarbeit mit dem Westbalkan realisiert werden. Vielmehr werden durch diese Kooperationsform im Rahmen der EU-Kooperation jährlich zehntausende Straftaten geklärt und tausende von gefahndeten Straftäterinnen und Straftätern und Terrorverdächtigen über Biometriedaten identifiziert. Damit können diese Personen justiziellen Strafverfahren zugeführt werden. Die Erfolgszahlen werden durch die Erweiterung der Prümer Zusammenarbeit auf die Westbalkanstaaten nochmals wesentlich steigen und die Westbalkanstaaten an höchste Datenschutzstandards herangeführt.

ABHILFEMASSNAHMEN (Art. 35 Abs. 7 lit. d DSGVO):

Innerhalb der Prümer Zusammenarbeit mit den Westbalkanstaaten wird die Datenübermittlung mit Unterstützung der Europäischen Kommission über das für den elektronischen Datenaustausch abgeschlossene EU-Kommunikationsnetzwerk TESTA eingeräumt. Die Verwendung von TESTA steht den Westbalkanstaaten im Rahmen der Prümer Zusammenarbeit zur Verfügung. Bei Nutzung des hochsicheren abgeschlossenen EU Hochleistungsnetzwerkes TESTA werden die für Suchanfragen übermittelten Biometriedaten entsprechend der Rechtstextvorgaben zusätzlich mit Prüm Verschlüsselungstechnologien, die nur von autorisierten Behörden entschlüsselt werden können, gegen ungerechtfertigten Datenzugriff abgesichert. An sich wird dieses Kommunikationsnetzwerk ausschließlich von EU-Mitgliedstaaten, EU-Agenturen und EU-Behörden, wie etwa der Europäischen Kommission oder dem Europäischen Parlament verwendet.

Auf Grund der besonderen Sensibilität des Vertragsgegenstandes wurden in dem Übereinkommen analog den angeführten Prümer-Beschlüssen dieselben Datenschutzstandards festgelegt. Diese Standards entsprechen in vollem Umfang den Bestimmungen der Prümer-Beschlüsse, welche die umfangreichsten und detailliertesten Datenschutzregelungen aller bisherigen Polizeikooperationsverträge innerhalb der EU enthalten. Diese zusätzlichen Datenschutzstandards des Übereinkommens sind vollinhaltlich als lex specialis Datenschutzbestimmungen, welche durch sehr detaillierte Dateninhalts-, Datensicherheits- und Datenprotokollierungsvorgaben über das allgemeine EU-Datenschutzregime der relevanten DSRL-PJ hinausgehen. Diese Bestimmungen der Prümer-Beschlüsse wurden im Übereinkommen inhaltsgleich unter Kapitel IV „Datenschutz“ (Art. 12 bis Art. 19) nachgebildet, womit auch die geforderten Garantien des EU-Datenschutzregimes für internationale Datentransfers mit höchstmöglicher Rechtssicherheit fixiert sind.

Vor Aufnahme eines operativen Datenaustausches sieht das Übereinkommen analog den Prüfprozessen ein umfassendes Test- und Prüfverfahren für neue Partnerstaaten in Art. 21 des Übereinkommens vor, so wie sie auch in der Prümer Zusammenarbeit rechtlich fixiert sind. In diesen Evaluierungsverfahren werden mit standardisierten Testdatensätzen, wie sie auch in der Prümer Zusammenarbeit verwendet werden, das Funktionieren aller Such- und Datenverarbeitungsprozesse kontrolliert und überprüft. Dieses

Verfahren wird von einem bereits operativen Prüm Partnerstaat auf Ersuchen eines zum Datenaustausch bereiten neuen Partnerstaates durchgeführt.

Nach erfolgreichem Abschluss der Testläufe wird eine Vorortprüfung im zu prüfenden Partnerstaat für jede einzelne Datenart vorgenommen. Hier werden unter anderem Datensicherheitsvorkehrungen, Zutrittsicherungen zu Rechen- und Forensikzentren geprüft und die Ergebnisse in Evaluierungsberichten dokumentiert.

Diese Evaluierungsberichte sind allen Vertragsstaaten des Übereinkommens in einer gemeinsamen Arbeitsgruppe vorzulegen (Art. 21 Abs. 2 des Übereinkommens). Der tatsächliche Datenaustausch mit einem neuen Partnerstaat wird aufgenommen, sobald alle Vertragsstaaten diesen Evaluierungsbericht entsprechend der Vertragsvorgaben angenommen haben und damit eine rechtskonforme Umsetzung bestätigen. Benutzungshandbücher enthalten administrative und technische Informationen für den effizienten und effektiven Datenaustausch (Art. 20 Abs. 2 des Übereinkommens).

Die übermittelten Daten werden – wie im Rahmen der Prümer Zusammenarbeit – nicht zentral oder in einem der abgefragten Partnerstaaten gespeichert, sondern verbleiben in den nationalen Datenbanken der abfragenden, datenbesitzenden Partnerstaaten, welche den im Übereinkommen verbindlich normierten Sicherheitsgarantien des aktuellen EU-Datenschutzregimes unterliegen.

Abgesehen von der datenschutzrechtlichen Protokollierungsspeicherung, für die nach zwei Jahren eine automatische Löschung vorgesehen ist, kommt es in den angeschlossenen Datenbanken der Partnerstaaten zu keinen wechselseitigen Speicherungen von Suchdatensätzen. Datensätze werden nur auf Übereinstimmung gesucht und nur im tatsächlichen Trefferfall biometrische Trefferdaten für erforderliche forensische Prüfprozesse und Verifizierungsprüfungen in den forensischen Administrativdatenbanken zur Erstellung von Gutachten weiterverarbeitet. Weiterführende personenbezogene Daten identifizierter Straftäterinnen und Straftäter oder von Falldaten dürfen nur im Falle forensisch bestätigter Treffer von den jeweiligen Partnerstaaten im Wege der definierten nationalen Zentralstellen angefordert und zwischen diesen Zentralstellen für die mögliche Einleitung von zielgerichteten kriminalpolizeilichen und justiziellen Ermittlungsverfahren bereitgestellt werden.

Zusammenfassend kann daher im Rahmen der Datenschutz-Folgenabschätzung bestätigt werden, dass keine großen datenschutzrechtlichen Risiken feststellbar und umfassende Vorkehrungen zur Prüfung rechtskonformer Umsetzung vorgesehen sind, bevor ein tatsächlicher Datenaustausch gestartet wird.