SWIFT

Mittwoch, 21 Oktober 2015

https://www.datenschutz.de/swift/

Nach einem zum 01.08.2010 in Kraft getretenen Abkommen zwischen der EU und den USA können letztere unter bestimmten Voraussetzungen auf Überweisungsdaten aus Europa zugreifen. Es geht hierbei um Überweisungen aus Europa in Drittstaaten. Inländische und innereuropäische (SEPA) Überweisungen sind nicht erfasst. Zuvor wurden die Daten jahrelang ohne hieb- und stichfeste Rechtsgrundlage übermittelt.

Die USA sind im Rahmen des Terrorist Finance Tracking Programs (TFTP) sehr an Finanztransaktionsdaten interessiert, weshalb sie von kurz nach den Anschlägen vom 11.09.2001 bis zum Jahreswechsel 2009/2010 über ein in den USA gelegenes Rechenzentrum des Finanzdienstleisters SWIFT (Society for Worldwide Interbank Financial Telecommunication) auf europäische Transaktionsdaten zugriffen. SWIFT ist eine internationale Genossenschaft von Geldinstituten mit Sitz in Belgien, die internationale Finanztransaktionen abwickelt. Die USA sind zunächst im Herbst 2001 mit der Bitte um Zugriff auf die im US-Rechenzentrum gespeicherten Daten nach US-Recht an SWIFT herangetreten. SWIFT gewährte den Zugang; die USA griffen auf Daten von Überweisungen von Europa ins außereuropäische Ausland zu. Sie konnten hierbei Informationen zu Absendern und Empfängern und zur Transaktionshöhe erhalten. Ermöglicht wurde dies durch die Architektur des SWIFT-Netzwerks. Es wurde aus zwei Rechenzentren in den Niederlanden und den USA betrieben, die ihren Inhalt jeweils spiegelten. Ein derartiges redundantes Vorgehen ist bei Systemen, die eine hohe Ausfallsicherheit bieten müssen, üblich.

Nachdem der Zugriff öffentlich bekannt wurde, kündigte SWIFT einen Umbau seiner IT-Architektur an, um den US-Zugriff zu beenden. Ein drittes Rechenzentrum in der Schweiz mit zwei voneinander getrennten Bereichen für europäische und amerikanische Daten sollte die Spiegelung der Bestände übernehmen. Europäische Daten waren damit nur noch in den Niederlanden und der Schweiz gespeichert, amerikanische in den USA und der Schweiz. Zum Jahreswechsel 2009/2010 ging das schweizer Rechenzentrum in Betrieb, ein direkter Zugriff für US-Behörden war damit nicht mehr möglich. In Einzelfällen konnten allerdings mittels eines 2003 geschlossenen Vertrages zur Rechtshilfe Informationen angefordert werden. Bereits im Sommer 2009 begannen Verhandlungen über ein Abkommen zur fortgesetzten Datenübermittlung, das zum 1.8.2010 in Kraft getreten ist, nachdem das Europäische Parlament zunächst eine erste Fassung abgelehnt hatte.

Das Abkommen erlaubt die Übermittlung von Transaktionsdaten zur Überweisungen ins außereuropäische Ausland, innereuropäische SEPA-Überweisungen (Single European Payment Area) sind von der Übermittlung ausgeschlossen. Die Zweckbindung des Abkommens beschränkt den Zugriff auf Anti-Terrorismus-Ermittlungen. Für die Abfragen gilt folgendes Vorgehen: Das TFTP übermittelt eine Anfrage mit einer Beschreibung der gewünschten Daten und Belegen für ihre Nützlichkeit für die Zwecke des Abkommens sowohl an den Finanzdienstleister, als auch an die europäische Polizeibehörde Europol. Diese Anfragen sollen „so eng wie möglich“ gefasst sein. Europol prüft dann die Begründetheit der Anfrage und gibt gegebenenfalls seine Zustimmung. Unabhängige Richter – wie in der Ablehunung

von Februar 2010 durch das Europäischen Parlament gefordert – werden nicht eingebunden. Aus technischen Gründen muss zudem immer ein Paket aus Finanztransaktionsdaten übermittelt werden; praktisch sieht es so aus, dass alle Überweisungen einer bestimmten Bank an einem bestimmten Tag übermittelt werden. Hierbei können Auftraggeber und Empfänger von Überweisungen samt ihren Kontonummern, Adressen und gegebenenfalls nationalen Identifikationsnummern übermittelt werden. Diese Pakete werden von den USA dann „geöffnet“ und die Informationen der verdächtigen Personen extrahiert. „Nicht-extrahierte“ Daten sollen für fünf Jahre gespeichert bleiben. Nach Angaben der US-Behörden selbst liefern 97% der übermittelten Daten keine Hinweise. Data-Mining in den übermittelten Daten und andere Techniken der automatischen Profilerstellung werden vom Abkommen ausgeschlossen. Das Abkommen gilt rückwirkend auch für Transaktionen, die in der Zeit vor dem Inkrafttreten durchgeführt wurden.

Das TFTP kann von sich aus Erkenntnisse aus den Daten an Europol, Eurojust und die nationalen Polizeibehörden der EU-Staaten übermitteln. Diese können sich ebenfalls an das TFTP wenden, um dort bereits übermittelte Daten durchsuchen zu lassen. Dies dürfte den Anreiz für Europol, die Übermittlung streng zu kontrollieren, einschränken. US-Behörden dürfen zudem aus den Daten gewonnene Erkenntnisse, nicht allerdings die Rohdaten selbst, an Drittstaaten weitergeben. Eine automatische Information der Betroffenen ist nicht vorgesehen, man kann jedoch bei den nationalen Datenschutzbehörden Auskunft über die Verwendung der Daten beantragen. Diese leiten die Anfrage dann an die zuständigen US-Behörden weiter, die eine Auskunft allerdings verweigern können. Bei Verdacht auf Missbrauch können EU-Bürger zudem Beschwerden bei den US-Behörden einlegen.

Zur Überprüfung des Abkommens sind gemeinsame Evaluationen vorgesehen. Es gilt zunächst für fünf Jahre und wird sich automatisch verlängern, sofern nichts anderes vereinbart wird. Die Kündigungsfrist beträgt sechs Tage. Auch wenn das Abkommen gekündigt werden sollte, können US-Behörden die bereits übermittelten Daten weiterhin nutzen. Das Abkommen enthält zudem eine Bestimmung, nach der die EU binnen drei bis fünf Jahren ein eigenes mit dem TFTP vergleichbares Analyseprogramm schaffen soll, wobei die USA mit Rat und Tat zur Seite stehen wollen.

Auch wenn das Abkommen umgangssprachlich als „SWIFT-Abkommen“ bezeichnet wird, gilt es auch für andere Transaktionsdienstleister.

Dieses Dossier wurde zusammengestellt von Herrn Langfeldt (ULD SH)
