

# Zu Gast bei Freunden? Übermittlung von Gewalttäter Sport-Datensätzen an russische Behörden im Zuge der WM 2018

 [juwiss.de/54-2018/](https://juwiss.de/54-2018/)

Gastautor

## JuWiss-Schwerpunktwoche zum Datenschutzrecht

von CHRISTOPHER GIOGIOS



Die Fußball-WM 2018 in Russland wirft bereits ihren Schatten voraus. Gemeint ist jedoch nicht die Debatte, ob nun Manuel Neuer oder Marc-André ter Stegen die Nr. 1 im deutschen Tor sein sollte; vielmehr soll es hier um die polizeiliche Übermittlung personenbezogener Daten an russische Behörden gehen. Details zur Übermittlung von Datensätzen aus der Datei „Gewalttäter Sport“ anlässlich des FIFA-Confederations-Cups 2017 wurden kürzlich durch Anfragen von Abgeordneten der Fraktion BÜNDNIS 90/DIE GRÜNEN publik. Ein guter Anlass also, um diesen Vorgang angesichts der bevorstehenden WM im Sommer 2018 genauer zu betrachten.

### Datei „Gewalttäter Sport“

Bei der Datei „Gewalttäter Sport“ handelt es sich um eine Verbunddatei auf Grundlage der §§ 11 I i.V.m. 2 I und III BKAG. Eine Verbunddatei wird von einer Zentralstelle (hier – wie auch in vielen anderen Fällen – das BKA) betrieben, die „Einspeisung“ von Daten erfolgt durch die abrufberechtigten Teilnehmer, d.h. vornehmlich durch Polizeibehörden der Länder. Wie der Name vermuten lässt, handelt es sich bei der DGS um eine Datei, die 2001 als Instrument für die Bekämpfung von Ausschreitungen im Zuge von Sportveranstaltungen errichtet worden ist. Dabei war bis 2010 umstritten, ob überhaupt eine taugliche Rechtsgrundlage für den Betrieb der Datei besteht. Gem. § 7 VI BKAG a.F. hätte durch das Bundesinnenministerium eine Verordnung über die Art der Daten erlassen werden sollen, die zulässigerweise in einer Verbunddatei gespeichert werden dürfen. Folglich stritt man darüber, ob diese Vorschrift deklaratorisch oder konstitutiv zu verstehen sei. Dankenswerterweise schuf das BMI jedoch Abhilfe und entwarf in erstaunlicher Geschwindigkeit eine entsprechende Verordnung, die nach Zustimmung des Bundesrates am 09.06.2010 in Kraft trat – am selben Tag, an dem eine mündliche Verhandlung vor dem Bundesverwaltungsgericht anstand, welche jene Rechtsfrage betraf. Dies könnte man durchaus als Punktlandung bezeichnen. Anders ausgedrückt: neun Jahre lang wurden ohne Ermächtigungsgrundlage in der DGS Personendaten gespeichert.

Zurück ins Jahr 2018. In einer kleinen Anfrage erkundigten sich die Bundestagsabgeordneten explizit nach der Übermittlung von Daten aus der DGS an die russische Grenzbehörde im Jahre 2017. Hierzu gab die Bundesregierung an, dass Bundespolizeibeamte Daten von fünf einreisenden Deutschen übermittelt hätten. Von

diesen sei zu erwarten gewesen, dass sie sich an Ausschreitungen beteiligen würden. Die Übermittlung an die russische Behörde sei mit der Maßgabe erfolgt, ein mögliches Einreiseverbot zu prüfen und diene ausschließlich der Gefahrenabwehr.

Als Rechtsgrundlage für die Datenübermittlung an ausländische Behörden durch die Bundespolizei sind die §§ 32, 33 BPolG heranzuziehen. Dabei sind zwei Aspekte zentral: die Erforderlichkeit der Übermittlung gem. § 32 III Nr. 2 BPolG sowie die Gegenüberstellung von schutzwürdigen Interessen des Betroffenen und dem öffentlichen Interesse an der Datenübermittlung gem. § 33 III BPolG.

## Erforderlichkeit der Datenübermittlung

---

Die Erforderlichkeit der Übermittlung dürfte weitgehend unproblematisch zu bejahen sein: die Bundesregierung verweist insofern auf die Abwehr erheblicher Gefahren gem. § 32 III Nr. 2 Alt. 1 (eine Legaldefinition findet sich in § 14 II 2 BPolG), also Gefahren für bedeutsame Rechtsgüter, welche hier etwa aufgrund der Möglichkeit (schwerer) Körperverletzungsdelikte wohl anzunehmen sind. Gleichwohl ließe sich diskutieren, ob im zeitlich so vorgelagerten Zeitpunkt der Einreise bereits die hinreichende Wahrscheinlichkeit eines Schadenseintritts gegeben ist und damit das Vorliegen einer Gefahr zu bejahen ist. Andernfalls wäre die Maßnahme auf § 32 III Nr. 2 Alt. 2 zu stützen, also der „Verhütung von Straftaten mit erheblicher Bedeutung“. Hierfür existiert jedoch im BPolG keine Legaldefinition, weshalb die Vorschrift vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG) hinsichtlich der Normenklarheit und Normenbestimmtheit aus Sicht des Betroffenen nicht unproblematisch ist. Das Bundesverfassungsgericht fordert in diesem Kontext die Zurechenbarkeit mindestens zum Bereich der mittleren Kriminalität, die empfindliche Störung des Rechtsfriedens sowie die Eignung der Straftat, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. Besser nachvollziehbar wäre hier gleichwohl – ähnlich wie im bayerischen PAG – ein Aufzählungskatalog; andernfalls bleibt es bei einer Einzelfallentscheidung durch Auslegung.

## Interessenabwägung / Angemessenheit des Datenschutzniveaus im Empfängerstaat

---

Interessanter ist jedoch die Regelung des § 33 III BPolG und das in S. 3 enthaltene Erfordernis eines „angemessenen Datenschutzniveaus“ im Empfängerstaat. Durch das Gegenüberstellen der schutzwürdigen Interessen des Betroffenen und des öffentlichen Interesses an der Datenübermittlung handelt es sich hier letztlich um eine Abwägungsentscheidung. Die grundsätzlichen Probleme dieser Vorschrift liegen auf der Hand: so ist fraglich, wie und nach welchen Maßstäben das Datenschutzniveau des Empfängerstaates im Einzelnen überprüft werden soll, um dem Recht auf informationelle Selbstbestimmung adäquat Rechnung zu tragen. Schon das Zusammentragen der einzelnen Vorschriften und deren Übersetzung dürften in der Praxis aufgrund des Zeitdrucks im Rahmen von Einzelfallentscheidungen schwer umsetzbar sein. Darüber hinaus schweigt das BPolG zum Maßstab der Angemessenheit des Schutzniveaus.

## Angemessenheitsbeschluss / Garantieerklärung nach der JI-Richtlinie

---

Abhilfe könnte allerdings Richtlinie EU 2016/680 („JI-Richtlinie“) schaffen, welche in den Art. 35 ff. allgemeine Grundsätze für die Datenübermittlung festlegt. Hierbei sieht Art. 36 für Übermittlungen an Drittstaaten die Möglichkeit eines sog. Angemessenheitsbeschlusses der Europäischen Kommission vor, in dessen Rahmen insbesondere nach den Kriterien des Art. 36 II die Angemessenheit des Schutzniveaus von Drittstaaten festgestellt werden kann. Ein solcher Beschluss liegt bislang für ein Dutzend Drittstaaten vor, nicht jedoch für die Russische Föderation.

Schließlich bleibt gem. § 33 III 4 BPolG die Möglichkeit, dass der Empfängerstaat für den Einzelfall einen angemessenen Umgang mit den Daten garantiert. Eine solche Garantie sei durch die russische Grenzschutzbehörde abgegeben worden – jedoch lediglich in Bezug auf die Löschung der Daten nach dem Turnier. Darüber hinaus ließe sich auch allgemein fragen, wie eine solche Garantieerklärung im Einzelfall auszusehen vermag und v.a., wie deren Einhaltung sichergestellt werden kann. Art. 37 I a) JI-RL fordert zwar ein „rechtsverbindliches Instrument“ für eine Garantie, Näheres zu deren konkreter Ausgestaltung findet sich hier jedoch nicht (Ähnliches lässt sich in Art. 46 der Datenschutz-Grundverordnung beobachten; auch hier werden lediglich weitere Rechtsformen aufgestellt, in deren Rahmen Garantien abgegeben werden können).

In der kleinen Anfrage verweist die Bundesregierung auf die russische Ratifikation der Konvention 108 des Europarats („Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“) aus dem Jahre 1981. Deren Ratifikation ist gemäß Erwägungsgrund 68 der JI-Richtlinie von der Kommission bei einem Angemessenheitsbeschluss (auch) zu berücksichtigen; hier allerdings soll die Datenschutzkonvention wohl als „rechtsverbindliches Instrument“ i.S.v. Art. 37 JI-RL verstanden werden.

Dazu soll gleichwohl nicht unbemerkt bleiben, dass dieses Vertragswerk an mehreren Stellen (s. nur Art. 9 II, auf den Russland in einer der Unterzeichnung beigefügten Erklärung explizit verweist) Ausnahmen von grundlegenden datenschutzrechtlichen Garantien vorsieht; insoweit ist die Bedeutung der europäischen Datenschutzkonvention für die Annahme eines angemessenen Datenschutzniveaus jedenfalls fraglich. Darüber hinaus darf nicht verkannt werden, dass selbst das Vorliegen eines Angemessenheitsbeschlusses die übermittelnden Behörden sowie die jeweiligen Kontrollinstanzen nicht davon entbindet, eine eigene Prüfung vorzunehmen und der Beschluss daher vielmehr als Entscheidungshilfe anzusehen ist – das gilt erst recht für eine Garantieerklärung.

Die Bundesbeauftragte für Datenschutz, Andrea Voßhoff (CDU), äußerte sich zu dem Vorgang nur insoweit, als dass sie eine „pauschale präventive“ Datenübermittlung ablehne und stattdessen auf eine Einzelfallprüfung abzustellen sei. Diese begrüßenswerte Auffassung wird jedoch dadurch relativiert, dass nach Überzeugung der Bundesregierung gerade aufgrund der im Rahmen grenzpolizeilicher Einreisekontrollen zu treffenden Einzelfallentscheidungen eine vorherige Befassung der Datenschutzbeauftragten der Länder und des Bundes nicht zu gewährleisten sei.

So oder so wird die Thematik weiter zu beobachten sein: für die Weltmeisterschaft im Sommer liegen bereits Datenübermittlungsersuchen russischer Sicherheitsbehörden vor.

Bleibt also (doch) die Ausgangsfrage nach der Nr. 1 im deutschen Tor. Zumindest hinsichtlich einer unproblematischen Einreise der Nationalmannschaft wäre wohl ter Stegen die klügere Wahl. Denn: Manuel Neuer musste sich bereits 2008 anlässlich der EM in Österreich und in der Schweiz beim Grenzübertritt einer mehrere Stunden andauernden Kontrolle unterziehen. Grund: ein Eintrag in der Datei Gewalttäter Sport.

**Zitiervorschlag:** Giogios, Zu Gast bei Freunden? Übermittlung von Gewalttäter Sport-Datensätzen an russische Behörden im Zuge der WM 2018, JuWissBlog Nr. 54/2018 v. 30.5.2018, <https://www.juwiss.de/54-2018/>



*Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.*