

Im Ergebnis hat der EuGH einer flächendeckenden, anlassbezogenen Reihenuntersuchung etwa in Fällen eines DNA-Abgleichs zur Identifizierung allfälliger Straftäter eine klare Absage erteilt. Selbst bei individuellem Tatverdacht verstoßen nationale Rechtsvorschriften, die die systematische Erhebung biometrischer und genetischer Daten aller Personen, die einer vorsätzlichen Officialstraftat beschuldigt werden, für die Zwecke ihrer Registrierung vorsehen, grds gegen die Anforderungen nach Art 10 JI-RL. Sie können nämlich unterschiedslos und allgemein zur Erhebung von Daten der meisten beschuldigten Personen führen (Rz 129 ff des Urteils).

Ausblick: Die äußerst bemerkenswerte Entscheidung des EuGH wird erhebliche Auswirkungen auf die Auslegung von § 39 DSGVO haben, der die Verarbeitung besonderer Kategorien personenbezogener Daten durch Polizei und Justiz, aber auch durch die Geheimdienste in Österreich regelt (näher zum Prüfungsschema *Thiele/Wagner*, DSGVO § 39 DSGVO Rz 32). Zumal der Begriff der „vorsätzlichen Officialstraftat“ (Rz 45 ff des Urteils) besonders allgemein gehalten ist und auf eine große Zahl von Straftaten, unabhängig von ihrer Art, ihrer Schwere, den besonderen Umständen dieser Straftaten, ihres etwaigen Zusammenhangs mit anderen laufenden Verfahren, den Vorstrafen der betroffenen Person oder deren individuellem Profil, angewendet werden kann. Für die Verarbeitung besonders kategorisierter Daten erfordert § 39 DSGVO neben einer ausreichend determinierten gesetzlichen Grundlage die *unbedingte* Erforderlichkeit (*Thiele/Wagner*, DSGVO § 39 DSGVO Rz 15 f). Das vorliegende Urteil hat den dafür nötigen Begründungsaufwand für die Sicherheitsbehörden deutlich gemacht.

Thematisch ergänzender Hinweis aus der österreichischen Rsp: Im Juni 2022 hat das BVwG (erst jüngst rechtskräftig) eine Verletzung im Grundrecht auf Geheimhaltung nach § 1 DSGVO bei einer Verarbeitung nach dem Dritten Hauptstück des DSGVO festgestellt. Denn die Staatsanwaltschaft hatte – entgegen § 74 StPO – keine ausreichenden Vorkehrungen getroffen und ua sensible Daten des Opfers (wie Name, Privatanschrift des Justizwachebeamten, Jahreskonto 2021 Justiz, private Handynummer, Geburtsdatum, Geburtsort, Lohnzettel inkl Zulagen, Personalnummer, Eintrittsdatum in die Justiz, Sozialversicherungsnummer, Krankenstandsdaten, Familienstand, Verletzungen, Behandlungsdaten und einen Unfallbericht der BVAEB) offengelegt (BVwG 21. 6. 2022, W292 2256548-1 [Unterlagen im Haftraum]).

Zusammenfassend hat der EuGH entschieden, dass die systematische Erhebung biometrischer und genetischer Daten aller beschuldigten Personen für die Zwecke ihrer polizeilichen Registrierung unzulässig ist. Diese – insb nach Art 10 JI-RL und Art 47 GRC zu beurteilende – Datenverarbeitung der Sicherheitsbehörden verstößt gegen die Anforderungen, einen erhöhten Schutz bei der Verarbeitung sensibler personenbezogener Daten zu gewährleisten.

Bearbeiter: Clemens Thiele

EuGH: Begründungspflicht für die Genehmigung von Telefonüberwachungen

» jusIT 2023/49

- § GRC: Art 7, 8, 47 Abs 2
RL 2002/58/EG: Art 5 Abs 1, Art 15 Abs 1
StPO: §§ 134 ff
TKG 2021: §§ 161 ff
- # EuGH 16. 2. 2023, C-349/21 (HYA u.a.)

- Art 15 Abs 1 ePrivacy-RL iVm Art 47 Abs 2 GRC steht einer nationalen Praxis, wonach gerichtliche Entscheidungen, mit denen auf einen ausführlichen mit Gründen versehenen Antrag der Strafverfolgungsbehörden hin die Anwendung besonderer Ermittlungsmethoden genehmigt wurde, nach einer Textvorlage abgefasst sind, die keine individualisierte Begründung enthält, sondern sich – abgesehen von der Angabe der Gültigkeitsdauer der Genehmigung – auf den Hinweis beschränkt, dass die Anforderungen der in diesen Entscheidungen angeführten Regelung erfüllt seien, nicht entgegen, sofern
 - die genauen Gründe, aus denen der zuständige Richter zu dem Ergebnis gelangt ist, dass die gesetzlichen Anforderungen unter den tatsächlichen und rechtlichen Umständen des konkreten Falls erfüllt seien, sich leicht und eindeutig erschließen, wenn die Entscheidung und der Antrag auf Genehmigung nebeneinander gelesen werden, und
 - dieser Antrag nach erteilter Genehmigung der Person zugänglich gemacht werden muss, gegenüber der die besonderen Ermittlungsmethoden genehmigt wurden.
- Die Verwertbarkeit von Beweismitteln, die gemäß innerstaatlichen Rechtsvorschriften entgegen den unionsrechtlichen TK-Überwachungsgrundsätzen erlangt wurden, unterliegt nach dem Grundsatz der Verfahrenautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung ua der Unionsgrundsätze von Äquivalenz und Effektivität – dem nationalen Recht.

Anmerkung des Bearbeiters:

In dem aus Bulgarien stammenden Ausgangsfall musste sich der EuGH letztlich mit den Anforderungen an die Begründung einer richterlichen Anordnung von TK-Überwachungsmaßnahmen befassen. Eine bulgarische Staatsanwaltschaft ermittelte gegen mehrere Beschuldigte. Darunter befanden sich ua auch drei Beamte der Grenzpolizei am Flughafen Sofia. Gegen sie bestand der Verdacht, Mitglieder in einer kriminellen Vereinigung zu sein, deren der Bereicherung dienendes Ziel es wäre, Drittstaatsangehörige über die



bulgarischen Grenzen einzuschleusen und in diesem Zusammenhang Bestechungsgelder anzunehmen oder zu zahlen.

In diesem Verfahren stellte die Strafverfolgungsbehörde beim Präsidenten des Spezialisierten Strafgerichts Bulgarien (*Spetsializiran nakazatelen sad*) jeweils detailliert begründete Anträge auf Telefonüberwachung, denen noch am Tag ihrer Einreichung stattgegeben wurde. Die richterlichen Genehmigungen beschränkten sich auf den Hinweis, dass die in den Anträgen angeführten Rechtsvorschriften eingehalten würden; Informationen zu den Tatvorwürfen enthielten sie dagegen nicht. Auch beinhalteten die Genehmigungen keine konkreten Umstände bzw Gründe dazu, aufgrund welcher Verdachtsumstände die Tatvorwürfe erhoben wurden. Die antragstellende Behörde wurde ebenfalls nicht genannt.

In der Folge wurde die Telekommunikation der Beschuldigten überwacht und schließlich aufgrund der auch dadurch gewonnenen Beweismittel die Anklage gegen sie erhoben. Das mit der Sache befasste Gericht legte das Verfahren dann dem EuGH mit der Frage vor, ob Unionsrecht einer nationalen Regelung entgegensteht, die Aufzeichnungen von Telefongesprächen gestattet, die durch eine nicht mit Gründen versehene gerichtliche Entscheidung genehmigt wurden. Der EuGH hatte auch zu klären, ob die so erlangten Beweismittel im Strafprozess verwendet werden dürften.

Die Dritte Kammer machte deutlich, dass grds die Entscheidung über die Genehmigung von Telefonüberwachung keine individualisierte Begründung enthalten muss, sofern der Verdächtige bzw Beschuldigte zumindest in der nachprüfenden richterlichen Kontrolle die tatsächliche und effektive Möglichkeit hat, den (sicherheitsbehördlichen bzw staatsanwaltschaftlichen) Antrag samt aller erforderlichen Informationen einzusehen, deren Inhalt sich die Beschlussbegründung zu eigen gemacht hat. Sobald also die betroffene Person darüber informiert wurde, dass ihr gegenüber besondere Ermittlungsmethoden angewandt wurden, verlangt jedoch die sich aus der Charta ergebende Begründungspflicht, dass diese Person in der Lage ist, die Gründe für die Genehmigung der Anwendung dieser Methoden nachzuvollziehen, damit sie diese Genehmigung gegebenenfalls sachdienlich und wirksam anfechten kann. Dieses Erfordernis gilt auch für jeden Richter, der nach Maßgabe seiner Befugnisse von Amts wegen oder auf Antrag der betroffenen Person die Rechtmäßigkeit der Genehmigung prüfen muss (Rz 51 ff des Urteils).

Der EuGH betonte, dass es Sache des vorlegenden Gerichts ist, zu prüfen, ob im Rahmen der fraglichen nationalen Praxis die Garantien von Art 7 und 8 GRC eingehalten und Art 15 ePrivacy-RL gewährleistet wurden, und ob sowohl die überwachten Personen als auch der Richter, der dafür zuständig ist, die Rechtmäßigkeit der Genehmigung der Überwachung zu prüfen, in der Lage sind, die Gründe für diese Genehmigung nachzuvollziehen. Das nationale Gericht hat insb darauf zu achten, ob und dass die überwachten Personen Zugang nicht nur zur Genehmigungsentcheidung haben, sondern auch zum Antrag, um diese „nebeneinander vergleichen“ zu können. Lassen sich nämlich, wenn der Antrag und die anschließende Genehmigung nebeneinander ge-

lesen werden, die Gründe für die Genehmigung nicht leicht und eindeutig nachvollziehen, so wäre festzustellen, dass die sich aus den genannten unionsrechtlichen Vorschriften ergebende Begründungspflicht verletzt ist (Rz 58 ff des Urteils).

Der EuGH klärt mit dem vorliegenden Urteil die nicht nur in Bulgarien, sondern auch in Deutschland oder Österreich gängige Praxis von Journal- oder Ermittlungsrichtern, ihre Entscheidungen nicht selbst zu verfassen, sondern letztlich nur von der Staatsanwaltschaft aus- bzw vorformulierte Entwürfe zu unterschreiben. Die Dritte Kammer hat einen Verstoß gegen das Unionsrecht verneint. Zwar verlange das durch Art 47 GRC garantierte Recht auf eine wirksame gerichtliche Kontrolle, dass der Betroffene Kenntnis von den Gründen einer ihm gegenüber ergangenen Entscheidung erlangen kann. Die wohl als Minimalanforderung zu bezeichnende Deckungsgleichheit zwischen begründetem TK-Überwachungsantrag und (begründungsloser) richterlicher Bewilligung genügen hier den sonst als besonders überwachungskritisch geltenden Höchststrichter:innen (vgl etwa EuGH 5. 4. 2022, C-140/20 [Commissioner of An Garda Síochána], *jusIT* 2022/62, 155 [Thiele] = *RZ* 2022/9 [Simma]; dazu *Kreul*, Nein, aber ... Die Vorratsdatenspeicherung in Europa, *MR-Int* 2022, 60). Die vorliegende Urteilsbegründung erinnert den aufmerksamen Rechtsanwender an so manches Strafurteil heimischer Prägung, worin – im Nachhinein – eine Handyüberwachung bestätigt wurde: Durch die Einsicht in den der Genehmigung der Abhörmaßnahme zugrunde liegenden Antrag (der freilich alle wesentlichen Informationen enthalten muss) könne der Betroffene die Gründe für die Maßnahme ohnehin nachvollziehen.

Zu beachten ist jedoch, dass diese Form der strafrichterlichen Aufwandserleichterung nur dann unionsrechtlich tragfähig bleibt, wenn die zugrunde liegenden Anträge der Strafverfolgungsbehörden iSv §§ 134, 136 StPO oder § 54 SPG alle für die Beurteilung der Rechtmäßigkeit der Maßnahme erforderlichen Informationen umfassen. Enthält der Antrag insoweit Lücken, ist das Gericht, wenn es die Voraussetzungen für die Anordnung einer strafprozessualen Maßnahme für gegeben hält, verpflichtet, die Gründe selbst in einer Ausführlichkeit darzulegen, die eine Überprüfung der Entscheidung an den Maßstäben von Art 47 GRC und Art 15 ePrivacy-RL ermöglicht.

Einmal mehr verweist das Höchstgericht die Frage der Zulässigkeit datenschutzwidrig erlangter Beweismittel in die Beurteilungskompetenz der vorlegenden Gerichte (vgl bereits EuGH 20. 9. 2022, C-793/19, C-794/19 [SpaceNet], *jusIT* 2022/93, 232 [Thiele]; zur österreichischen Rechtspraxis *Thiele/Wagner*, *DSG*² § 1 Rz 196 mwN).

Ausblick: Gewissermaßen weiterführend bzw verwandt zur entschiedenen Thematik stellt sich in einem österreichischen Vorlageverfahren an den EuGH die Frage nach den unionsrechtlichen Bedingungen, die Polizeibehörden erfüllen müssen, um Zugang zu den auf einem Mobiltelefon einer Person gespeicherten Daten zu erhalten, wenn gegen den Mobiltelefoneigentümer ein strafrechtliches Ermittlungsverfahren geführt wird (Rs C-548/21 [C.G. gegen BH Landeck]). Nach den bereits vorliegenden Schlussanträgen (GA Campos Sánchez-Bordona 20. 4. 2023,

C-548/21, Rz 105) bedarf es auch dazu einer vorherigen richterlichen Anordnung, die in ihrer Begründung auf die Schwere der Anlasstat sowie auf die unbedingte Erforderlichkeit und das Verhältnismäßigkeitsprinzip Rücksicht nimmt. Im Rahmen einer strafrechtlichen Ermittlung dürfen die Polizeibehörden nicht in Eigeninitiative und ohne vorherige gerichtliche Anordnung umfassenden und unkontrollierten Zugang zu allen auf einem Mobiltelefon gespeicherten Daten erhalten, wenn sich daraus ein genaues Bild des Privatlebens der betroffenen Person gewinnen lässt.

Zusammenfassend hat der EuGH entschieden, dass eine richterliche Entscheidung, mit der eine Telekommunikationsüberwachung genehmigt wird, gem Art 15 Abs 1 ePrivacy-RL iVm Art 47 Abs 2 GRC dann keine individualisierte Begründung enthalten muss, wenn ihr ein ausführlich begründeter Antrag der zuständigen Strafverfolgungsbehörde zugrunde liegt und sich die für die Anordnung der Maßnahme ausschlaggebenden Gründe leicht und eindeutig erschließen. Dafür genügt es, dass die Entscheidung und der Genehmigungsantrag nebeneinander gelesen werden und einander ergänzen.

Bearbeiter: Clemens Thiele

EuGH: Keine Erheblichkeitsschwelle für Anspruch auf immateriellen Schadenersatz bei Datenschutzverstößen

» jusIT 2023/50

§ VO (EU) 2016/679: Art 82 Abs 1, ErwGr 146 Satz 3
EuGH 4. 5. 2023, C-300/21 (Österreichische Post)

1. Die bloße Verletzung einer Bestimmung der DSGVO per se begründet keinen Schadenersatzanspruch.
2. Der Ersatz eines immateriellen Schadens gebührt unabhängig davon, ob dieser einen bestimmten Grad an Erheblichkeit erreicht hat.
3. Die Bemessung der Höhe des Schadenersatzes richtet sich nach nationalem Recht, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten sind.

Anmerkung der Bearbeiterin:

Der EuGH hat erstmals über die – heftig umstrittene – Frage entschieden, unter welchen Voraussetzungen ein Anspruch auf immateriellen Schadenersatz bei Datenschutzverletzungen gem Art 82 Abs 1 DSGVO besteht. Die Besprechung des mit Spannung erwarteten Urteils erfolgt durch *Sonja Janisch* in Heft 4/2023.

Bearbeiterin: Sonja Janisch

EuGH: Recht auf Kopie kann auch Dokumente umfassen

» jusIT 2023/51

§ VO (EU) 2016/679: Art 15 Abs 3 Satz 1 und Satz 3
EuGH 4. 5. 2023, C-487/21 (Österreichische Datenschutzbehörde)

1. Das in Art 15 Abs 3 DSGVO verbrieftete Recht, bei Ausübung des Auskunftsrechts eine „Kopie“ der personenbezogenen Daten zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion der Daten auszufolgen ist.
2. Das Recht auf Erhalt einer Kopie umfasst die Bereitstellung von Auszügen aus Dokumenten oder von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die diese verarbeiteten Daten enthalten, wenn dies unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DSGVO verliehenen Betroffenenrechte zu ermöglichen.
3. Der unionsautonome Begriff der „Informationen“ in Art 15 Abs 3 Satz 3 DSGVO bezieht sich ausschließlich auf personenbezogene Daten, von denen der für die Verarbeitung Verantwortliche gem Satz 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

Anmerkung des Bearbeiters:

Über den österreichischen Ausgangsfall im Zusammenhang mit einer Auskunftsanfrage an die österreichische CRIF wurde an dieser Stelle bereits berichtet (*Thiele*, jusIT 2021/93, 253). Nunmehr liegen die Antworten zu den Vorlagefragen des BVwG (9. 8. 2021, W211 2222613-2 [Recht auf Kopie]) vor. Der EuGH hatte sich im Kern damit zu beschäftigen, was das Recht, eine „Kopie“ der personenbezogenen Daten zu erhalten, umfassen kann bzw darf.

Nach Auffassung der Ersten Kammer bedeutet das Recht auf eine „Kopie“ der verarbeiteten personenbezogenen Daten iSv Art 15 Abs 3 Satz 3 DSGVO, dass die betroffene Person eine originalgetreue und verständliche Reproduktion aller dieser Daten erhält. Dieses Recht impliziert aber auch das Recht auf eine Kopie von Auszügen aus Dokumenten/Datenbanken oder gar von ganzen Dokumenten, die diese Daten enthalten. Vorausgesetzt ist, dass diese Auszüge unerlässlich sind, um die erforderliche Transparenz und leichte Verständlichkeit der Informationen zu gewährleisten und der betroffenen Person so die wirksame Ausübung der ihr durch die DSGVO verliehenen Rechte zu ermöglichen. Die Kopie muss daher alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind (Rz 32 des Urteils). Insbesondere wenn personenbezogene Daten aus anderen Daten generiert werden oder wenn sie auf freien Feldern beruhen, also einer fehlenden Angabe, aus der eine Information über die betroffene Person hervorgehe, ist nach Ansicht des EuGH der Kontext, in dem diese Daten, die Gegenstand der