C-252/21 ([Meta Platforms u.a.], jusIT 2023/88, 200 [*Thiele*] = ÖJZ 2023/143, 876 [*Fuchs*]) mit der Frage zugestellt hat, ob dieser unter Berücksichtigung dieses Urteils sein Vorabentscheidungsersuchen ganz oder teilweise aufrechterhalten wolle. Daraufhin hat der OGH seine erste und dritte Vorlagefrage zurückgenommen und seine zweite und vierte Vorlagefrage aufrechterhalten.

Inhaltlich geht es im nun ergangenen Urteil zunächst um die Frage, ob die Verarbeitung personenbezogener Daten von Facebook-Nutzern durch Meta Platforms Ireland mit dem Grundsatz der Datenminimierung des Art 5 Abs 1 lit c DSGVO vereinbar ist. Dabei werden durch Meta Platforms Ireland sowohl innerhalb als auch außerhalb dieses sozialen Netzwerks ua Daten über den Abruf der Onlineplattform sowie von Websites und Anwendungen Dritter erhoben und auch das Navigationsverhalten der Nutzer auf diesen Seiten mittels Social Plug-ins und Pixels, die auf den betreffenden Websites eingefügt werden, verfolgt. Der EuGH sieht darin einen schweren Eingriff in die Grundrechte der betroffenen Person. Diese Art von Verarbeitung ist besonders umfassend, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta Platforms Ireland aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird. Daher ist es nach dem Grundsatz der Datenminimierung unzulässig, dass der Betreiber eines sozialen Netzwerks sämtliche personenbezogenen Daten, die er von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet.

Die zweite Fragestellung betrifft Art 9 Abs 2 lit e DSGVO, wonach eine Ausnahme vom Verarbeitungsverbot sensibler Daten dann besteht, wenn die betroffene Person diese Daten selbst öffentlich gemacht hat. Im konkreten Fall hat *Max Schrems* bei einer öffentlich zugänglichen Podiumsdiskussion, die per Streaming übertragen und zudem als Podcast und über einen Youtube-Kanal veröffentlicht wurde, Angaben zu seiner sexuellen Orientierung gemacht. In weiterer Folge erhielt er regelmäßig Werbung, die auf ein homosexuelles Publikum abzielte, und Einladungen zu entsprechenden Veranstaltungen, obwohl er sich zuvor für diese Veranstaltungen nicht interessiert hatte und den Veranstaltungsort nicht kannte. Der EuGH entschied, dass diese Äußerung von *Max Schrems* über seine sexuelle Orientierung im Rahmen einer öffentlichen Podiumsdiskussion Facebook nicht berechtigt, weitere Daten über seine sexuelle Orientierung zu sammeln und für personalisierte Werbung zu verarbeiten. Die Ausnahmeregelung des Art 9 Abs 2 lit e DSGVO ist eng auszulegen, sodass auch nach einer öffentlichen Aussage keine automatische Einwilligung für weiter gehende Datenverarbeitungen vorliegt. Der EuGH stellte zwar fest, dass es nicht auszuschließen ist, dass die Äußerung bei der Podiumsdiskussion eine Handlung darstellt, mit der der Betroffene in voller Kenntnis der Sachlage seine sexuelle Orientierung iSv Art 9 Abs 2 lit e DSGVO offensichtlich öffentlich gemacht hat. Dies berechtigt allerdings den Betreiber eines sozialen Netzwerks nicht, andere Daten über die sexuelle Orientierung dieser Person zu verarbeiten, die er gegebenenfalls außerhalb dieser Plattform von Anwendungen und Websites dritter Partner im Hinblick darauf erhalten hat, sie zu aggregieren und zu analysieren, um dieser Person personalisierte Werbung anzubieten.

Zusammengefasst stellt der EuGH in diesem Urteil klar, dass eine unbegrenzte und umfassende Datensammlung und -verarbeitung über Facebook-User durch Meta Platforms Ireland unverhältnismäßig ist und gegen den Grundsatz der Datenminimierung verstößt. Zudem berechtigt die Öffentlichmachung der sexuellen Orientierung bei einer öffentlichen Podiumsdiskussion nicht zur Verarbeitung weiterer Daten über die sexuelle Orientierung dieser Person für Werbezwecke.

Bearbeiter: Dietmar Jahnel

EuGH: Polizeilicher Zugriff auf Smartphones unterliegt strengen Voraussetzungen

» jusIT 2024/180

§ GRC: Art 7, 8, 47, 52 Abs 1
RL (EU) 2016/680: Art 1, 2 Abs 1, Art 3 Z 2, Art 4 Abs 1 lit c, Art 6, 10, 13, 54
RL 2002/58/EG: Art 1 Abs 1 und 3, Art 3, 5, 15
DSG: §§ 36, 37
SMG: § 27 Abs 1
StGB: § 17
StPO: § 18 Abs 1, § 99 Abs 1, § 110 Abs 3

\# EuGH 4. 10. 2024, C-548/21 (BH Landeck – Versuchter Zugriff auf persönliche Daten, die auf einem Mobiltelefon gespeichert sind)

1. Art 4 Abs 1 lit c RL (EU) 2016/680 erlaubt es den zuständigen Behörden, zum Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten grds auf Daten zuzugreifen, die auf Mobiltelefonen gespeichert sind. Dieser Zugriff ist jedoch nur zulässig, wenn die betroffene Straftat klar definiert ist, der Grundsatz der Verhältnismäßigkeit gewahrt wird und – außer in dringenden Fällen – eine vorherige Überprüfung durch ein Gericht oder eine unabhängige Stelle erfolgt.
2. Art 13 und 54 RL (EU) 2016/680 untersagen eine nationale Regelung, die es den Behörden ermöglicht, ohne Benachrichtigung der betroffenen Person auf Mobiltelefondaten zuzugreifen, wenn diese Benachrichtigung keine Beeinträchtigung der behördlichen Aufgaben mehr darstellt. Die betroffene Person ist darüber zu informieren, sobald die Gefährdung der Aufgaben entfällt, insb über die Gründe, auf denen die richterliche oder behördliche Genehmigung beruht.

Anmerkung des Bearbeiters:

Der aus Österreich stammende Ausgangsfall befasst sich ganz grds mit den Grenzen und Voraussetzungen für den Zugang der Polizei zu persönlichen Daten, die auf Mobiltelefonen gespeichert sind.

Der Sachverhalt spielt in Tirol und spiegelt den Alltag der Strafrechtspraxis wider: Ein deutscher Saisonier am Arlberg, der später Betroffene, erhob eine Maßnahmenbeschwerde gegen die Sicherstellung seines Mobiltelefons im Zuge einer Hausdurchsuchung in seiner Unterkunft durch die Kriminalpolizei im Zuge von Ermittlungen aufgrund eines an ihn adressierten Briefes mit Cannabiskraut. Zum Zeitpunkt der Durchsuchung lag für die gesetzten Maßnahmen weder eine Anordnung der Staatsanwaltschaft noch ein gerichtlicher Beschluss vor. Das nach Art 130 Abs 1 Z 2 B-VG zuständige LVwG Tirol hatte Bedenken gegen die Rechtmäßigkeit der Handy-Beschlagnahme und leitete ein Vorabentscheidungsersuchen an den EuGH ein. Es wollte zusammengefasst wissen, ob das dem Beschwerdeführer im strafgerichtlichen Ermittlungsverfahren zur Last gelegte Vergehen nach § 27 Abs 1 SMG im Lichte der Unionsrechtsprechung zu Art 15 Abs 1 ePrivacy-RL überhaupt eine so weitreichende Auswertung eines Mobiltelefons, welche den völlig unkontrollierten Zugang zur gesamten digitalen Kommunikation des Betroffenen eröffnet, rechtfertigen könnte. Die zweite Frage zielte darauf ab, ob insb aus grundrechtlichen Erwägungen iSv Art 7, 8 GRC eine Handy-Sicherstellung ohne vorausgegangene richterliche Anordnung zulässig ist. Schließlich sollte die dritte Vorlagefrage klären, ob unter dem Aspekt der Waffengleichheit und eines wirksamen Rechtsbehelfes iSv Art 47 GRC eine nach der Beschlagnahme erfolgte digitale Auswertung eines Mobiltelefons durch die Sicherheitspolizei rechtmäßig ist, wenn der Betroffene weder vorher noch zumindest nach Setzung der Maßnahme davon informiert wurde; dies unter Berücksichtigung der Vorgaben von Art 4 Abs 1 lit c, Art 13 und 54 Abs 1 RL (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 Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89 (kurz: JI-RL).

Die Große Kammer folgt dem Schlussantrag von GA *Campos Sánchez-Bordona* (SA 20. 4. 2023, Rs C-548/21) und betont, dass der Zugriff auf alle Daten, die auf einem Mobiltelefon gespeichert sind, zwar einen schwerwiegenden oder sogar besonders schwerwiegenden Eingriff in das Privatleben derjenigen darstellt, deren Handy ausgewertet wird. Dennoch würde eine ausschließliche Beschränkung dieser Zwangsmaßnahme auf Fälle schwerer Kriminalität die Ermittlungsbehörden zu sehr beschränken. Neben dem Grundsatz der Verhältnismäßigkeit ist jedenfalls auch jener der Datenminimierung gem Art 4 Abs 1 lit c JI-RL maßgeblich zu beachten. Die Handysicherstellung muss klar „*gesetzlich vorgesehen*“ sein (Rz 85 des Urteils). Der EuGH hält es für unverzichtbar, die Betroffenen über die Gründe zu informieren, die den Zugriff auf die Daten rechtfertigen, sobald diese Information die Ermittlungen nicht mehr beeinträchtigen kann. Bei sichergestellten Handys muss das idR sogar schon vor dem Zugriffsversuch auf die abgespeicherten Daten geschehen (Rz 120 des Urteils).

Der Eingriff in die in Art 7 und 8 GRC verbürgten Rechte ist daher sogar als besonders schwerwiegend einzustufen. Demzufolge muss der Zugang zu den auf Mobiltelefonen gespeicherten Daten durch die zuständigen Polizeibehörden verweigert oder eingeschränkt werden, wenn unter Berücksichtigung der Schwere der Straftat und des Untersuchungszwecks ein Zugang zu Kommunikationen oder sensiblen Daten nicht gerechtfertigt erscheint. Die Schwere der Straftat bleibt ein zentraler Parameter bei der Prüfung der Verhältnismäßigkeit, aber nicht der allein ausschlaggebende. Entgegen einigen Missdeutungen des Richterspruchs aus Luxemburg (vgl *LTO-Redaktion*, Polizei-Zugriff auf Handydaten: EuGH gegen pauschale Beschränkung auf schwere Kriminalität, in Legal Tribune Online, 4. 10. 2024, <https://www.lto.de/persistent/a_id/55561> [11. 11. 2024]) macht die Große Kammer nämlich mehrere ganz klare Vorgaben für nationale Gesetzgeber, die sich anschicken, die Handysicherstellung schon bei Delinquenz mit geringer Strafdrohung als probates Mittel polizeilichen Handelns routinemäßig zu gestatten:

- Zunächst sind die Kriterien für den Grundrechtseingriff, insb die Art oder die Kategorien der betreffenden Straftaten, hinreichend präzise festzulegen („*alle Vergehen und Verbrechen*“ wird den Determinierungsanforderungen nicht gerecht).
- Die gesetzlich determinierte Sicherstellungsregelung hat zu enthalten, dass zwischen verschiedenen Kategorien betroffener Personen (Verdächtige, [potenzielle] Opfer einer Straftat, andere) und deren Datenbetroffenheit zu unterscheiden ist.
- Jedenfalls, und das verhilft der Maßnahmenbeschwerde im Anlassfall letztlich zum Erfolg, müssen Beschlagnahme und Auswertung der nationalen Behörden, maW der zwangsbewehrte Zugang zu personenbezogenen Daten auf dem sichergestellten Mobiltelefon – außer in klar begründeten Fällen hoher Dringlichkeit – von einer vorherigen Kontrolle durch ein Gericht (oder eine unabhängige Verwaltungsstelle) abhängig gemacht werden.

Abschließend macht der EuGH ganz deutlich, dass die einschlägige RL zum Datenschutz in Strafsachen gem Art 1 Abs 1 iVm Art 3 Z 2 JI-RL nicht nur gilt, wenn die Polizei tatsächlich an die Daten auf einem sichergestellten Handy herankommt, sondern auch dann, wenn sie den Versuch dazu unternimmt (Rz 104 des Urteils).

Das umfangreiche Urteil lässt sich in seinen einzelnen Aussagen und Vorgaben an den nationalen Gesetzgeber bzw die Vollzugsbehörden wie folgt zusammenfassen:

1. Der Zugriff der Polizei auf Mobiltelefondaten kann grds nicht ausschließlich auf die Bekämpfung schwerer Kriminalität beschränkt werden. Ein Zugriff ist jedoch nur nach vorheriger Genehmigung durch eine unabhängige Behörde oder nach vorheriger richterlicher Anordnung zulässig, außer in dringenden, hinreichend begründeten Fällen.
2. Der Zugriff auf Mobiltelefondaten muss verhältnismäßig sein, da dieser einen schwerwiegenden Eingriff in die Grundrechte der betroffenen Personen darstellt. Die Schwere des Eingriffs ergibt sich durch die sensible Natur der Daten und deren Rückschlüsse auf das Privatleben.

3. Die Mobiltelefondaten erlauben detaillierte Einblicke in das Privatleben, darunter die persönliche Kommunikation, Fotos und der Internetverlauf, die teils hochsensible Informationen enthalten können. Solche Eingriffe bedürfen daher besonderer Schutzmechanismen.
4. Nationale Gesetzgeber sind verpflichtet, klare und präzise Regelungen für den Zugriff auf Mobiltelefondaten zu schaffen. Dabei sind insb die Straftatkategorien und sonstigen Zugriffsbedingungen festzulegen, um die Eingriffsintensität auf ein erforderliches Maß zu begrenzen.
5. Betroffene Personen müssen nachträglich über die Gründe und den Umfang des Zugriffs auf ihre Daten informiert werden, sobald dies die laufenden Ermittlungen nicht mehr gefährdet. Dies stärkt das Recht auf Transparenz und individuelle Rechte der betroffenen Personen.
6. Der Schutzbereich von Art 3 iVm Art 4 Abs 1 lit c JI-RL erstreckt sich auch auf erfolglose Zugriffsversuche auf die Daten, was den Schutz personenbezogener Daten und die Rechte der betroffenen Personen erheblich erweitert.

Ausblick: Besondere Bedeutung haben die Ausführungen des EuGH für die hierzulande anstehende Reform der Handydaten-Sicherstellung. Die dem Gesetzgeber aufgegebene Reparaturfrist läuft am 31. 12. 2024 aus (VfGH 14. 12. 2023, G 352/2021 [Handysicherstellung], ZIIR 2024, 34 [*Thiele*] = ecolex 2024/113, 194 [*Soyer/Marsch*] = JBl 2024, 166 [*Reindl-Krauskopf*] = AnwBl 2024/87, 164 [*Soyer/Marsch*] = AnwBl 2024/88, 168 [*Moser/Kodek*] = AnwBl 2024/58, 112 [*Dietachmair*] = ZWF 2024, 2 [*Rohregger*] = ZWF 2024/6, 31 = MR 2024, 25 [*Brandstetter*] = JSt-Slg 2024/4 [*Hollaender*] = JSt 2024, 118 [*Soyer/Marsch*] = ÖJZ 2024/72, 471 [*Schumann*]). Ein Blick auf den Kern des Sachverhalts verdeutlicht die Tragweite des vorliegenden Urteils: Die Polizei versuchte, ein im Rahmen einer Drogenfahndung sichergestelltes Mobiltelefon zu entsperren. Dies geschah ohne richterliche Genehmigung und ohne den Besitzer zu informieren. Der EuGH sieht in diesem Vorgehen einen möglichen Verstoß gegen die JI-RL zum Schutz personenbezogener Daten durch Maßnahmen der Strafverfolgungsbehörden. Die Große Kammer betont, dass eine vorherige Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle zwingend erforderlich ist, um einen gerechten Ausgleich zwischen den Erfordernissen der Strafverfolgung und den Grundrechten auf Privatsphäre und Datenschutz zu gewährleisten. Der nationale Gesetzgeber ist daher unter erheblichem Zugzwang, das österreichische Beschlagnahmerecht rasch verfassungs- und unionsrechtskonform anzupassen – am 32. Dezember ist es zu spät!

Zusammenfassend hat der EuGH entschieden, dass sich der Zugang der Polizei zu auf Mobiltelefonen gespeicherten personenbezogenen Daten nicht nur auf die Bekämpfung schwerer Kriminalität beschränken muss, die Grundsätze der Verhältnismäßigkeit und der Datenminimierung aber jedenfalls zu berücksichtigen sind. Eine richterliche Anordnung – selbst für den Versuch des Datenzugangs – stellt eine unverzichtbare Rechtmäßigkeitsvoraussetzung dar.

Bearbeiter: Clemens Thiele

EuGH: Weitergabe von Daten der Mitglieder eines Sportverbandes an Sponsoren

» jusIT 2024/181

§ VO (EU) 2016/679: Art 5 Abs 1 lit a, Art 6 Abs 1 lit f

EuGH 4. 10. 2024, C-621/22 (Koninklijke Nederlandse Lawn Tennisbond)

1. Der Begriff „*berechtigte Interessen*“ in Art 6 Abs 1 lit f DSGVO ist nicht auf gesetzlich festgelegte Interessen beschränkt, sondern umfasst auch wirtschaftliche Interessen.
2. Die Offenlegung personenbezogener Daten der Mitglieder eines Sportverbands gegen Entgelt aus wirtschaftlichem Interesse des Verbandes ist nur dann zur Wahrung der berechtigten Interessen erforderlich, wenn die Verarbeitung zur Verwirklichung des berechtigten Interesses absolut notwendig ist und sofern in Anbetracht aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten der Mitglieder demgegenüber nicht überwiegen.

Anmerkung des Bearbeiters:

In dieser Entscheidung des EuGH geht es um die Frage, ob die Offenlegung personenbezogener Daten der Mitglieder eines niederländischen Tennisverbands an zwei Sponsoren ohne Einwilligung der Betroffenen zulässig war. Bei einem der Sponsoren handelte es sich um eine Gesellschaft, die Sportartikel vertreibt, beim anderen um den größten Anbieter von Glücks- und Casinospielen in den Niederlanden. Diese Datenweitergabe, für die der Tennisverband ein Entgelt erhielt, erfolgte zum Zweck der Ermöglichung von Werbemaßnahmen der Sponsoren. Umfasst waren in beiden Fällen Namen, Anschriften und Wohnorte der Mitglieder; dem Glücksspielanbieter wurden darüber hinaus Geburtsdaten, Festnetznummern, Mobiltelefonnummern und E-Mail-Adressen übermittelt.

Die niederländische Datenschutzbehörde verhängte gegen den Tennisverband eine Geldbuße iHv € 525.000 wegen Verstoßes gegen die DSGVO, da keine Einwilligung der Mitglieder für die Datenverarbeitung vorlag und kein berechtigtes Interesse anerkannt wurde.

Der Tennisverband erhob gegen diese Entscheidung Klage mit der Begründung, dass die Offenlegung der Daten auf einem berechtigten Interesse gem Art 6 Abs 1 lit f DSGVO basierte. Dieses Interesse bestehe zum einen darin, eine enge Verbindung zwischen dem Verband und seinen Mitgliedern herzustellen, und zum anderen darin, diesen einen Mehrwert für die Mitgliedschaft in Form von Preisnachlässen und Angeboten bei Partnern bieten zu können. Damit soll den Mitgliedern ermöglicht werden, Tennis zu einem günstigen und erschwinglichen Preis zu betreiben. Die niederländische Datenschutzbehörde vertrat demgegenüber