

der Argumentationsaufwand für die Begründung derartiger, eher als alltäglich einzustufender Datenverarbeitungen im öffentlichen Bereich ist. Weil nach Art 6 Abs 1 UAbs 2 DSGVO Verarbeitungen von Behörden in Erfüllung ihrer Aufgaben nicht auf berechnete Interessen gem Art 6 Abs 1 lit f DSGVO gestützt werden können, muss dafür eine gesetzliche Grundlage iSd Art 6 Abs 1 lit e DSGVO gefunden werden. Dabei stößt man gerade (aber nicht nur) im Bereich der Schulen auf die Problematik, dass Datenverarbeitungen auf Webseiten, Social-Media-Plattformen oder im Zusammenhang mit dem Anfertigen von Fotos in den infrage kommenden gesetzlichen Grundlagen für die Wahrnehmung von Aufgaben im öffentlichen Interesse nicht explizit geregelt sind. Auch wenn das Ergebnis durch das BVwG sehr sorgfältig argumentiert wurde, bleibt eine gewisse Unsicherheit bei der Auslegung des Rechtfertigungstatbestandes, weshalb das BVwG mE völlig zu Recht die ordentliche Revision an den VfGH zur Frage zugelassen hat, ob § 56 SchUG eine Rechtsgrundlage iSd Art 6 Abs 1 lit e bzw Abs 3 lit b DSGVO darstellt. Offen ist zudem die Frage, ob derartige abstrakt formulierte Rechtsgrundlagen für Verarbeitungen im öffentlichen Bereich mit § 1 Abs 2 DSG und

dem Bestimmtheitsgebot des Art 18 Abs 1 B-VG unter Berücksichtigung von Art 6 Abs 3 DSGVO vereinbar sind. Mit diesen Fragen wird sich der VfGH über kurz oder lang zu befassen haben.



Der Autor:

Dr. **Dietmar Jahnel** ist ao. Univ.-Prof. am Fachbereich Öffentliches Recht der Universität Salzburg mit den Forschungsschwerpunkten Datenschutzrecht und Rechtsinformatik und ua Vortragender des Universitätslehrgangs für Informations- und Medienrecht an der Universität Wien.

Publikationen des Autors (Auswahl):

Neben zahlreichen Zeitschriftenbeiträgen Autor bzw Herausgeber von zuletzt Kommentar zur DSGVO (2021) unter Mitarbeit von *Christian Bergauer*, Jahrbuch Datenschutzrecht 2021, Lehrbuch Datenschutzrecht (3. Auflage 2021) gemeinsam mit *Angelika Pallwein-Prettner*.

✉ Dietmar.Jahnel@plus.sbg.ac.at

🌐 lesen.lexisnexus.at/autor/Jahnel/Dietmar

Foto: Foto Veigl

DATENSCHUTZ & E-GOVERNMENT JUDIKATUR

DATENSCHUTZRECHT

EuGH: Datenspeicherung in Testdatenbank nur vorübergehend zulässig

» jusIT 2022/92

§ VO (EU) 2016/679: Art 5 Abs 1 lit b und e, Art 6 Abs 1 lit a und Abs 4, Art 32

EuGH 20. 10. 2022, C-77/21 (Digi)

1. Der Grundsatz der Zweckbindung nach Art 5 Abs 1 lit b DSGVO steht einer separaten Speicherung personenbezogener Daten in einer internen zusätzlichen Datenbank (hier: eines TV- und Internetanbieters) nicht entgegen, sofern dies zum selben Zweck (hier: Verfügbarkeit der Kundenabonnements nach technischer Störung) erfolgt oder mit diesen Zwecken iSv Art 6 Abs 4 DSGVO vereinbar ist. Die Beweislast für die Zweckkompatibilität liegt beim Verantwortlichen.
2. Aus einer Zusammenschau von Art 5 Abs 1 lit b, Art 6 Abs 1 lit a und Art 6 Abs 4 DSGVO ergibt sich, dass sich die Frage der Vereinbarkeit der Weiterverarbeitung personenbezogener Daten mit den Zwecken, für die sie ursprünglich erhoben wurden, nur stellt, wenn die Zwe-

cke dieser Weiterverarbeitung nicht mit denen der ursprünglichen Erhebung übereinstimmen.

3. Der Grundsatz der Speicherbegrenzung nach Art 5 Abs 1 lit e DSGVO macht es aber erforderlich, dass eine Test- oder Sicherungsdatenbank (zur Behebung einer technischen Anomalie und der vorübergehenden Sicherung der personenbezogenen Daten) nach dem Zeitraum, in dem die Behebung vollständig durchgeführt wurde (dh mit Zweckerreichung), zu löschen ist. Eine nachlaufende Speicherung von 18 Monaten ist jedenfalls unzulässig.

Anmerkung des Bearbeiters:

In dem aus Ungarn stammenden Ausgangsfall erhielt einer der führenden Internet- und Fernsehanbieter dieses Landes, die Digi Távközlési és Szolgáltató Kft. (kurz: Digi), eine Geldbuße von umgerechnet ca € 250.000 von der ungarischen Datenschutzbehörde. Digi hatte nämlich im Anschluss an eine technische Servorstörung eine Testdatenbank erstellt und darin die personenbezogenen Daten von etwa einem Drittel seiner Privatkund:innen kopiert, um Tests durchzuführen und Fehler beheben zu können. Diese Datensätze waren ursprünglich für den Zweck des Abschlusses von Abonnementverträgen erhoben worden. Einem „ethischen Hacker“ gelang es aber, auf die Testdatenbank zuzugreifen, sodass die näheren Umstände im Rahmen einer Sicher-

heitsmeldung (*data breach notification*) publik wurden. Nach Ansicht der ungarischen DSB hätte Digi diese Datenbank nach der Durchführung der notwendigen Tests und Fehlerbeseitigungen längst löschen müssen. Tatsächlich wurde die Testdatenbank noch 18 Monate lang weiterbetrieben. Vor dem Budapester Gerichtshof bekämpfte Digi die Geldbuße; schließlich legte das Gericht die Sache nach Luxemburg vor. Der EuGH hatte sich ua damit zu befassen, ob überhaupt und ggf wie lange wegen einer Serverstörung die Kund:innendaten in einer zusätzlichen Datenbank gespeichert werden dürfen.

Die Erste Kammer bejahte die Zulässigkeit des Überspielens der Datensätze in eine Testdatenbank aufgrund des technischen Defekts, maW das Sicherheits-Back-up, denn es war vom Zweckbindungsgrundsatz des Art 5 Abs 1 lit b DSGVO gedeckt. Dem Verantwortlichen war es gestattet, in einer zu Testzwecken und zur Behebung von Fehlern eingerichteten Datenbank personenbezogene Daten zu erfassen und zu speichern, die zuvor erhoben und in einer anderen Datenbank gespeichert wurden, wenn diese Weiterverarbeitung mit den konkreten Zwecken vereinbar ist, für die die personenbezogenen Daten ursprünglich erhoben worden waren, was anhand der in Art 6 Abs 4 DSGVO genannten Kriterien und sämtlicher Umstände fallkonkret zu beurteilen ist. Die konkrete Weiterverarbeitung zur Fehlerbehebung und zu Testzwecken erfüllte die Kriterien (Rz 43 und 44 des Urteils). Hingegen hielt der EuGH das Belassen der Datensätze nach Durchführung der Tests und der Fehlerbehebung für weder mit dem Grundsatz der Speicherbegrenzung noch der Datenminimierung für vereinbar. Ist nämlich der Zweck der Verarbeitung weggefallen, hat der Verantwortliche umgehend zu löschen (Rz 53 und 61 des Urteils).

Zuzustimmen ist dem vorliegenden Urteil zunächst darin, dass ein fehler- oder wartungsbedingtes Ausweichen auf eine Test- oder Sicherheitsdatenbank vom ursprünglichen Verarbeitungszweck der Datensätze umfasst ist. Die Durchführung von Tests und die Behebung von Fehlern, welche die Qualität der Abonnementkundendatenbank beeinträchtigen, weisen einen konkreten Zusammenhang mit der Erfüllung der mit den Fernseh- und Internetteilnehmenden abgeschlossenen Verträge auf. Denn solche Fehler können sich nachteilig auf die Erbringung der vertraglich abonnierten Dienstleistungen auswirken, für die die Daten ursprünglich erhoben wurden. Diese Verarbeitung weicht nicht von den legitimen Erwartungen der Abonnent:innen hinsichtlich der weiteren Verwendung ihrer Daten ab. Gleichermäßen erscheint die strikte Beschränkung der Speicherdauer zu treffend. Die Grundsätze der Zweckbindung und der Speicherbegrenzung gelten kumulativ, dh, die Speicherung personenbezogener Daten muss nicht nur dem Grundsatz der „Zweckbindung“, sondern auch dem Grundsatz der „Speicherbegrenzung“ genügen. Aus Letzterem folgt, dass selbst eine ursprünglich zulässige Verarbeitung von Daten im Laufe der Zeit mit der DSGVO unvereinbar werden kann, wenn diese Daten für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, nicht mehr erforderlich sind. Sobald also der Grund für das Ausweichen bzw der Sicherungszweck durch die erfolgreiche Wiederherstellung der ursprünglichen Datenbank weggefallen ist, müs-

sen die Datensätze von der Testdatenbank gelöscht werden (so bereits EuGH 7. 5. 2009, C-553/07 [Rijkeboer] Rz 33, jusIT 2009/74, 151 [Jahnel]; EuGH 24. 9. 2019, C-136/17 [GC ua Auslistung sensibler Daten] Rz 74, Dako 2021/49, 90 [Haidinger/Löffler] = jusIT 2019/74, 210 [Staudegger] = jusIT 2019/91, 245 [Thiele] = ÖJZ 2019/130, 1102 [Kumin/Maderbacher]). Damit konkretisiert das Urteil zugleich die Anforderungen bei der Löschung von Daten und zeigt insb die Notwendigkeit des Führens eines Nachweises der erfüllten Löschpflicht auf (zur praktischen Umsetzung eines Löschkonzepts vgl Thiele, Datenschutz auf der Großbaustelle – Zur Teilnahme an Personaldokumentationssystemen aus Sicht der DSGVO, in Jahnel [Hrsg], Datenschutzrecht. Jahrbuch 2018 [2018] 151).

Ausblick: Das vorliegende Urteil erweitert sehr praxistauglich die Möglichkeiten der Wartung und (teilweisen) Wiederherstellung von Datenbanksystemen, die personenbezogene Daten enthalten, ebenso wie der kurzzeitigen Speicherung auf externen Servern zu Sicherungszwecken. Damit dürfte auch die Weiterverarbeitung zu Zwecken der Anonymisierung zulässig sein (instruktiv zum technischen Hintergrund Sonntag, Technische Grenzen der Anonymisierung, jusIT 2018/54, 137 mwH).

Zusammenfassend hat der EuGH entschieden, dass ein Internet- und Fernsehdiensteanbieter auch ohne die Einwilligung der Kund:innen bei einer Serverstörung deren Daten in einer externen Datenbank speichern darf, allerdings nur so lange, wie die Störung andauert. Ist der Zweck der Weiterverarbeitung und Speicherung weggefallen, muss unverzüglich gelöscht werden.

Bearbeiter: Clemens Thiele

EuGH: Zu Zulässigkeit und Grenzen der Vorratsdatenspeicherung

» jusIT 2022/93

§ GRC: Art 7, 8, 11, 52 Abs 1
EMRK: Art 8
RL 2002/58/EG: Art 15 Abs 1
RL 2003/6/EG: Art 12
VO (EU) 596/2014: Art 23
TKG (Deutschland): §§ 113a–113e
StPO (Deutschland): §§ 100g, 101a

EuGH 20. 9. 2022, C-793/19, C-794/19 (SpaceNet und Telekom Deutschland)
EuGH 20. 9. 2022, C-339/20, C-397/20 (VD und SR)

1. Zu den verbundenen Rs C-793/19, C-794/19 (Deutschland):

- a) Die verdachtsunabhängige Speicherung von IP-Adressen, Standort- und Verbindungsdaten aller Nutzerinnen und Nutzer, so wie sie im dTKG (in §§ 113a–113e idF dBGBI 2004 I, 1190) verankert wurde, widerspricht Art 15 Abs 1 ePrivacy-RL 2002/58/EG und ist insgesamt unionsrechtswidrig.