

auf die Entscheidung folgenden Fall veranlasst, die ordentliche Revision zuzulassen, was den OGH zur Bekräftigung seiner Vorentscheidung veranlasste:

Der OGH hat sein Verständnis einer öffentlich zugänglichen Datei präzisiert bzw von der Vorentscheidung abstrahiert: Für die öffentliche Zugänglichkeit einer Datei ist es nicht erforderlich, dass »jedermann« im wörtlichen Sinne Einsicht in eine bestimmte Datei nehmen könne. Es reiche vielmehr aus, dass es einen entsprechend großen Kreis an Abfrageberechtigten gibt und das berechnete Interesse an der Einsichtnahme im Einzelfall nicht überprüft wird.

Hinzuweisen ist an dieser Stelle auf die gesetzgeberische Reaktion und auf die als gefestigt anzusehende Judikatur: Mit BGBl I 2010/28 wurde das Verbraucherkreditgesetz erlassen, in dessen § 7 Abs 5 die Anwendbarkeit des § 28 Abs 2 DSG auf bei der DSK registrierte Informationsverbundsysteme kreditgebender Institutionen zur Bonitätsbeurteilung, bei denen die Verwendung auf § 8 Abs 1 Z 2 (Zustimmung des Betroffenen) oder Z 4 (überwiegende berechnete Interessen eines anderen) DSG beruht, ausgeschlossen wurde. Die Warnliste und die Kleinkreditevidenz wurden damit gezielt aus dem Anwendungsbereich des § 28 Abs 2 DSG »befreit«.

III. Zum Lösungsanspruch gemäß § 27 DSG

A. OGH 2.7.2009, 6 Ob 78/08a Verfügungsgewalt über Datenträger, Beschlagnahme

Entgegen den Bestimmungen des DSG verarbeitete Daten sind vom Auftraggeber gemäß § 27 Abs 1 DSG grundsätzlich zu löschen, und zwar aus eigenem, sobald die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, und sonst auf begründeten Antrag des Betroffenen.

Mit einer kuriosen Wendung in Zusammenhang mit einem Lösungsbegehren hatte der Oberste Gerichtshof sich in einem Revisionsverfahren auseinanderzusetzen: Die Datenträger, auf denen sich die behaupteterweise unzulässig verarbeiteten Daten befanden, waren nicht länger im Gewahrsam des Anspruchsgegners, sondern waren

gemäß § 143 StPO (aF) noch vor Erhebung des Löschungsbegehrens strafgerichtlich beschlagnahmt worden. Dadurch wurde die Frage aufgeworfen, ob durch die Nichtvornahme der Löschung durch den Auftraggeber eine Verletzung im Recht auf Löschung eingetreten war.

Der OGH hält dazu fest, dass eine behauptete Rechtsverletzung dann vorliege, wenn der Betroffene geltend mache, dass sein Antrag auf Löschung nach § 27 Abs 1 Z 2 DSG entweder nicht (innerhalb der Frist des § 27 Abs 4 DSG) erledigt worden sei (Säumnis) oder die ihm über seinen Antrag zugegangene negative Mitteilung, warum die verlangte Löschung nicht vorgenommen wurde, rechtswidrig sei. Eine Verletzung im Recht auf Löschung sei daher nur dann möglich, wenn der Betroffene ein Löschungsbegehren nach § 27 Abs 1 Z 2 DSG an den Auftraggeber gerichtet hätte.

Ein solches Löschungsbegehren war im gegenständlichen Fall auch tatsächlich erhoben worden – nur war der Auftraggeber schon zu diesem Zeitpunkt nicht mehr in Besitz der Datenträger, auf denen sich die zu löschenden Daten befanden. Infrage käme deshalb allenfalls eine Rechtsverletzung infolge Säumigkeit.

Allerdings, wie der Gerichtshof hervorhebt, setzt die Erledigung eines Löschungsanspruchs des Betroffenen die Verfügungsgewalt des Auftraggebers über die davon betroffenen Daten voraus. Es hätte einen Bruch der Beschlagnahme und eine unzulässige Veränderung der Beweismittel bedeutet, hätte der Beklagte dem Löschantrag entsprochen. Seine mangelnde Verfügungsgewalt über die vom Löschantrag betroffenen Daten der Kläger hinderte ihn an der Erledigung des Löschantritts.

Durch seine Säumigkeit hat er daher das Recht der Kläger auf Löschung nicht verletzt; der Beklagte bleibt jedoch zur Löschung verpflichtet und hat diese – säumnisfrei – vorzunehmen, sobald sich die betroffenen Datenträger wieder in seiner Verfügungsgewalt befinden.

B. VwGH 25. 11. 2008, 2005/06/0301 Schwärzung, Protokollbuch, Papierakt, Dokumentation

Ein Löschungsbegehren mit menschenrechtlicher Dimension hat den Verwaltungsgerichtshof gleich mehrmals beschäftigt:

Der Beschwerdeführer war nach § 209 StGB (aF) verurteilt worden, ein Delikt, das der Europäische Gerichtshof für Menschenrechte in der

Folge für unvereinbar mit den Garantien der Menschenrechtskonvention erkannte. Die Verurteilung wurde gemäß § 363 a StPO vom Obersten Gerichtshof aufgehoben, der Straftatbestand mit BGBl I 2002/ 134 aus dem österreichischen Rechtsbestand ausgeschieden. Allerdings befanden sich weiterhin automationsunterstützt und nicht automationsunterstützt verarbeitete personenbezogene Daten des Beschwerdeführers bei den Gendarmeriedienststellen, die die Ermittlungen wegen des Verdachts der Begehung der Straftat geführt hatten.

Der Beschwerdeführer hatte in seinem an die belangte Behörde gerichteten Löschungsbegehren die Unzulässigkeit der (weiteren) Verarbeitung seiner strafverfahrensbezüglichen Daten ins Treffen geführt, da diese nicht mehr für sicherheitspolizeiliche bzw strafjustizielle Zwecke benötigt würden. Dem Antrag auf Löschung insbesondere der im Protokollbuch eines Gendarmeriepostens und in der elektronischen Datenanwendung »AVTN« enthaltenen Daten wurde unter Hinweis auf die Notwendigkeit interner Dokumentation jedoch nicht entsprochen.

Der Verwaltungsgerichtshof hatte nun allerdings bereits entschieden, dass derartige Protokollbucheintragungen bestimmungsgemäß dazu dienen, den Geschäftsfall zu konkretisieren und den Akt auffinden zu können. Sie seien daher der behördeninternen Kanzleitätigkeit zu Dokumentationszwecken zuzuordnen. Es sei aber im Anlassfall eine Interessensabwägung vorzunehmen. Konkret seien vor dem Hintergrund des verurteilenden Erkenntnisses des Gerichtshofes für Menschenrechte, der Aufhebung der Verurteilung durch den Obersten Gerichtshof und der Streichung des einschlägigen Straftatbestandes die Argumente, die für eine Löschung sprechen, gewichtiger, als jene, auf welche die belangte Behörde den angesprochenen Dokumentationszweck gestützt hätte. Daher komme die Löschung der betreffenden Eintragungen in Betracht.

Die Löschung des Namens des Beschwerdeführers könne im Protokollbuch durch Schwärzung, in der elektronischen Datenanwendung AVTN durch Entfernung vorgenommen werden. Dadurch werde die Verknüpfung der Eintragung mit der Person des Beschwerdeführers derart unterbrochen, dass der Papierakt personenbezogen, dh mit dem Namen des Beschwerdeführers, nicht mehr auffindbar sei. Angesichts dessen sei davon auszugehen, dass die Zugänglichkeit (Erkennbarkeit) der den Beschwerdeführer betreffenden Daten im Papierakt derart reduziert werde, dass von einem Eingriff in das aus Art 8 EMRK erfließende Recht auf Achtung des Privatlebens nicht mehr die Rede sein könne.

**C. VwGH 23. 11. 2009, 2008/05/0079 Schwärzung,
Vernichtung, Protokollbuch, Papierakt, Datei**

Diese Gedanken hat der Verwaltungsgerichtshof in einem wenig später folgenden Erkenntnis wiederholt und ausgebaut: Für Protokollbucheintragungen stellt er nochmals klar, dass diese bestimmungsgemäß der Konkretisierung des Geschäftsfalles und der Auffindbarkeit des Aktes dienen und damit der behördeninternen Kanzleitätigkeit zuzurechnen sind. Gleiches gilt für Steckzettel, Indexkarteikarten und die elektronischen Aktendokumentationssysteme AVTN und AMKO.

Ein Recht auf »Vernichtung« eines Papieraktes ist dem Gesetz indessen nicht zu entnehmen. Schwärzung ist, wie bereits zuvor ausgeführt, eine Form der Löschung und für Papierakten ausreichend.

Zur Dateiqualität eines konventionellen, etwa bei einem Gendarmereiposten befindlichen Papieraktes merkt er an, dass dieser mangels entsprechender Strukturierung bzw eines gewissen Organisationsgrades typischerweise keine Datei iSd DSG darstellt.

**D. VfGH 16. 12. 2009, B 298/09 Papierakt, Datei,
PAD, Interessenabwägung, § 13 Abs 2 SPG**

In diesem Punkt der datenschutzrechtlichen Qualifikation von Papierakten besteht völlige Übereinstimmung mit der vom Verfassungsgerichtshof vertretenen Auffassung, der in einem rezenten Erkenntnis in sicherheitspolizeilichem Zusammenhang ebenfalls festgestellt hat, dass Kopie- bzw Papierakten nicht als Dateien iSd § 4 Z 6 DSG zu qualifizieren sind. Daran ändere auch der Umstand nichts, dass das EDV-System PAD nicht länger nur »äußere Daten« wie Namen des Betroffenen und das angezeigte Delikt, sondern nunmehr auch »innere Daten« wie Vernehmungsprotokolle enthalten würde.

Von Interesse sind vor allem die weitergehenden Ausführungen des Verfassungsgerichtshofes, die er zum EDV-System PAD und dessen gesetzlicher Grundlage getätigt hat:

Nach § 13 Abs 2 SPG bestehe eine Ermächtigung für Sicherheitsbehörden, sich bei der Wahrnehmung ihrer gesetzlichen Aufgaben zur Dokumentation von Amtshandlungen und der Verwaltung von Dienststücken der automationsunterstützten Datenverarbeitung zu bedienen. Zu diesen Zwecken dürften sie Daten über natürliche und juristische