Verwaltungsgericht Aachen

§ 3 a Abs. 2 PAuswG
(Speicherung von Daten beim Besuch)

Für die Erhebung und Speicherung der maschinenlesbaren Ausweis- oder Passdaten von Besuchern besteht keine Rechtsgrundlage.
(Verwaltungsgericht Aachen, Beschluss vom 18. Juni 2008 – 8 K 2513103)

Tatbestand:

Der Kläger wendet sich gegen das in der Justizvollzugsanstalt Aachen (JVA) seit Ende des Jahres 2000 übliche Verfahren, seine persönlichen Daten beim Betreten der Anstalt – wie bei allen Besuchern –vom Personalausweis oder Reisepass maschinell abzulesen und zu speichern. Ferner begehrt er die Löschung der bisher auf diese Weise gespeicherten Daten . . .

Entscheidungsgründe:

Die Klage hat Erfolg.

Der Verwaltungsrechtsweg ist gegeben. Nach § 40 Abs. 1 Verwaltungsgerichtsordnung (– VwGO –) ist der Rechtsweg zu den Verwaltungsgerichten in allen öffentlich-rechtlichen Streitigkeiten nichtverfassungsrechtlicher Art eröffnet, soweit diese nicht durch Bundesgesetz einem anderen Gericht ausdrücklich zugewiesen sind. Es handelt sich hier um eine öffentlich-rechtliche Streitigkeit nichtverfassungsrechtlicher Art. Gestritten wird um die Anwendung einer öffentlich-rechtlichen Norm, nämlich um § 3 a Abs. 2 PAuswG (bzw. § 17 Abs. 2 PassG), der die Zulässigkeit einer Datenspeicherung beim automatischen Lesen von Personalausweisen regelt.

Die Streitigkeit ist nicht durch Bundesgesetz einem anderen Gericht ausdrücklich zugewiesen (§ 40 Abs. 1 Satz 1 VwG0, „soweit“). Sie hat insbesondere keinen Justizverwaltungsakt im Sinne des § 23 EGGVG zum Gegenstand. Nach § 23 Abs. 1 EGGVG entscheiden die ordentlichen Gerichte über die Rechtmäßigkeit der Anordnungen, Verfügungen oder sonstigen Maßnahmen, die von den Justizbehörden zur Regelung einzelner Angelegenheiten auf den Gebieten des bürgerlichen Rechts einschließlich des Handelsrechts, des Zivilprozesses, der freiwilligen Gerichtsbarkeit und der Strafrechtspflege getroffen werden. Das gleiche gilt für Anordnungen, Verfügungen oder sonstige Maßnahmen der Vollzugsbehörden im Vollzug der Untersuchungshaft sowie derjenigen Freiheitsstrafen und Maßregeln der Besserung und Sicherung, die außerhalb des Justizvollzuges vollzogen werden. Eine Streitigkeit auf einem dieser Gebiete liegt nicht vor, insbesondere geht es nicht um eine Maßnahme im Vollzug der Untersuchungshaft. Unmittelbarer Streitgegenstand ist die Auslegung und Anwendung des § 3a PAuswG, der nicht zu den von § 23 Abs. 1 EGGVG erfassten Gebieten gehört. Es handelt sich hierbei vielmehr um eine bereichsspezifische Datenschutzregelung. Zwar kann der Zweck des Besuchs einer JVA, für den der Beklagte das Hergeben und die Bereitschaft zum automatischen Auslesen und zum Speichern von Personalausweisdaten verlangt – wie im Fall des Klägers das Aufsuchen eines Untersuchungsgefangenen sein. Das führt aber nicht dazu, dass die nicht im Haftrecht angesiedelte, unmittelbar streitbefangene Norm zu einer solchen des Untersuchungshaftrechts wird bzw. kraft eines weiten Zusammenhangs diesem Bereich zuzurechnen ist, für den die ordentlichen Gerichte zuständig wären. Gleiches gilt für einen etwaigen geplanten Besuch eines Strafgefangenen und die Zuständigkeit der Strafvollstreckungskammer gemäß § 109 Abs. 1 Satz 1 StVollzG. Dabei ist auch zu berücksichtigen, dass § 23 EGGVG wegen seines Ausnahmecharakters eng auszulegen ist, vgl. v. Albedyll in: Bader, VwGO-Kommentar, 3. Aufl., § 40 Rdnr. 98 mit Rechtsprechungsnachweis.

Die Klage ist als Leistungsklage auch sonst zulässig. Eines Vorverfahrens bedurfte es nicht, weil § 68 VwGO für allgemeine Leistungsklagen nicht einschlägig ist. Der Kläger begehrt die Unterlassung eines bestimmten Verhaltens (Unterlassungsklage als Unterfall der Leistungsklage) sowie die Löschung von Daten (Leistungsklage).

Die Klage ist auch begründet.

Der Kläger hat einen Unterlassungsanspruch (Klageantrag zu 1.) und einen Anspruch auf Datenlöschung (Klageantrag zu 2.).

Die in der JVA Aachen geübte Praxis ist rechtlich nicht erlaubt. Sie bedürfte einer gesetzlichen Grundlage. Eine solche gibt es nicht.

Die Verwendung der maschinenlesbaren Ausweis- oder Passdaten eines Ausweisinhabers bzw. Passinhabers stellt einen Eingriff in dessen Recht auf „informationelle Selbstbestimmung“ dar. Das Bundesverfassungsgericht (BVerfG) hat mit seinem„Volkszählungsurteil“ vom 15. Dezember 1983, – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440183 –, BVerfGE 65, 1, BGBl 11984, 31, NJW 1984, 419, DVBl 1984, 128, DOV 1984, 156, DVBl 1984, 385, klargestellt, dass unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst wird. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu. bestimmen (Recht auf „informationelle Selbstbestimmung“). Einschränkungen dieses Rechts sind nur im überwiegenden Allgemeininteresse zulässig und bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen

muss. In dieser Entscheidung hat das Bundesverfassungsgericht weiter ausgeführt (Rdnr. 147), dass dieses Recht unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes bedarf. Eine hohe Gefährdung liegt vor allem darin, dass bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, sondern heute vielmehr mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Eine weitere Besonderheit liegt darin, dass personenbezogene Daten darüber hinaus mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden können, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert.

Unter anderem in seinem Urteil vom 20. November 2007, – 1 BvR 1254/07DVBl 2008, 575, NJW 2008, 1505, DuD 2008, 352, zur automatisierten Kennzeichenerfassung von Fahrzeugen, mit dem es die dort angegriffenen Vorschriften als Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung eingestuft hat, hat das Bundesverfassungsgericht diese Argumentation aufgegriffen und vertieft. In der Entscheidung führt es aus, dass durch die elektronische Datenverarbeitung eine Gefährdungslage bereits im Vorfeld konkreter Bedrohungen von Rechtsgütern entstehen kann. Eine Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt nach den Worten des Gerichts in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte. Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene erforderliche Grundrechtsschutz.

Die danach erforderliche gesetzliche Rechtsgrundlage für die hier streitbefangene Verwendung der maschinenlesbaren Ausweis- oder Passdaten von Ausweisinhabern bzw. Passinhabern, die die JVA Aachen besuchen wollen, gibt es nicht. Die Handhabung der JVA ist insbesondere nicht nach § 3 a Abs. 2 PAuswG (oder der gleichlautenden Vorschrift des § 17 Abs. 2 PassG) erlaubt. § 3 a PAuswG regelt (u. a.) die Voraussetzungen der Nutzung der auf der Vorderseite enthaltenen maschinenlesbaren Zone des Personalausweises (und des Reisepasses). Er lautet wie folgt:

„**(1)** Behörden und sonstige öffentliche Stellen dürfen den Personalausweis nicht zum automatischen Abruf personenbezogener Daten verwenden. Abweichend von Satz 1 dürfen die Polizeibehörden und -dienststellen des Bundes und der Länder sowie, soweit sie Aufgaben der Grenzkontrolle wahrnehmen, die Zollbehörden den Personalausweis im Rahmen ihrer Aufgaben und Befugnisse zum automatischen Abruf personenbezogener Daten verwenden, die für Zwecke

1.
der Grenzkontrolle,

2.
der Fahndung oder Aufenthaltsfeststellung aus Gründen der Strafverfolgung, Strafvollstreckung oder der Abwehr von Gefahren für die öffentliche Sicherheit im polizeilichen Fahndungsbestand geführt werden. Über Abrufe, die zu keiner Feststellung geführt haben, dürfen, vorbehaltlich gesetzlicher Regelungen nach Absatz 2, keine personenbezogenen Aufzeichnungen gefertigt werden.

(2) Personenbezogene Daten dürfen, soweit gesetzlich nichts anderes bestimmt ist, beim automatischen Lesen des Personalausweises nicht in Dateien gespeichert werden; dies gilt auch für Abrufe aus dem polizeilichen Fahndungsbestand, die zu einer Feststellung geführt haben."

Um einen nur bestimmten Behörden erlaubten Abruf nach Abs. 1 der Vorschrift geht es vorliegend nicht. Abruf bedeutet nämlich, dass mit Hilfe des automatischen Auslesens Daten aus anderen Datenbanken (polizeilicher Fahndungsbestand) erschlossen, also Daten daraus durch das Auslesen erschlossen werden, im Einzelnen dazu Sailmuth/Koch, Erl. zu § 3 a PAuswG, Rdnr. 17 ff., ebenso die Kommentierung von Ehmann/Brunner, Pass- und Ausweisrecht, zu § 17 PassG.

Vielmehr geht es vorliegend um das in § 3 a Abs. 2 PAuswG geregelte Speichern beim automatischen Lesen. Inhaltlich bestimmt die Vorschrift, dass beim automatischen Lesen des Ausweises gewonnene Daten ausschließlich unter den Voraussetzungen des § 163 d StPO in Dateien gespeichert werden dürfen. Der § 163 d StPO ist nämlich die einzige Norm, die im Sinne der Ausnahmeklausel „soweit gesetzlich nichts anderes bestimmt ist" innerhalb der Verbotsnorm des § 3 a Abs. 2 PAuswG eine Speicherung beim Lesen zulässt.

Diese Bedeutung der Norm erschließt sich aus einem Blick auf ihre Vorgeschichte. Nach Einführung der Maschinenlesbarkeit der Ausweise durch das 4. Änderungsgesetz zum PAuswG vom 25. Februar 1983, siehe hierzu die Beschlussempfehlung und Bericht des Innenausschusses, BT-Drs. 8/3498, wurde § 3 a PAuswG durch das 5. Änderungsgesetz vom 19. April 1986, vgl. Gesetzentwurf, BT-Drs. 10/2177, geltendes Recht.

Mit dem 5. Änderungsgesetz zum PAuswG sollten ausdrücklich „die nach dem Volkszählungsurteil des Bundes-

verfassungsgerichts veranlassten datenschutzrechtlichen Ergänzungen" vorgenommen werden. § 3 a Abs. 2 der Entwurfsfassung enthielt allerdings noch 5 Absätze. Sein Abs. 2 lautete zu Beginn:

„Personenbezogene Daten dürfen beim automatischen Lesen des Personalausweises nicht in Dateien gespeichert werden. Abweichend von Satz 1 dürfen Polizeibehörden des Bundes und der Länder … Abrufe: aufzeichnen, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass dies

1.
zur Aufklärung einer der in § 100a der Strafprozessordnung genannten. Straftaten oder

2.
zur Verhütung einer solchen unmittelbar drohenden Straftat führen kann…"

Gesetz wurde er mit folgendem Wortlaut:
„Personenbezogene Daten dürfen, soweit gesetzlich nichts anderes bestimmt ist, beim automatischen Lesen des Personalausweises nicht in Dateien gespeichert werden; dies gilt auch für Abrufe aus dem polizeilichen Fahndungsbestand, die zu einer Feststellung geführt haben."
Der Gesetzgeber fügte also den Zusatz „soweit gesetzlich nichts anderes bestimmt ist" ein und verschob den (auf die in § 100 a StPO genannten Straftaten bezogenen) Rest der Entwurfsvorschrift einschließlich der Abs. 3–5 in ein anderes Gesetz, nämlich in einen neuen § 163 d StPO („Schleppnetzfahndung"). Dieser lautet:
„**(1)** Begründen bestimmte Tatsachen den Verdacht, dass

1.
eine der in § 111 bezeichneten Straftaten oder

2.
eine der in § 100a Abs. 2 Nr. 6 bis 9 und 11 bezeichneten Straftaten begangen worden ist, so dürfen die anlässlich einer grenzpolizeilichen Kontrolle, im Falle der Nummer 1 auch die bei einer Personenkontrolle nach § 111 anfallenden Daten über die Identität von Personen sowie Umstände, die für die Aufklärung der Straftat oder für die Ergreifung des Täters von Bedeutung sein können, in einer Datei gespeichert werden, wenn Tatsachen die Annahme rechtfertigen, dass die Auswertung der Daten zur Ergreifung des Täters oder zur Aufklärung der Straftat führen kann und die Maßnahme nicht außer Verhältnis zur Bedeutung der Sache steht. Dies gilt auch, wenn im Falle des Satzes 1 Pässe and Personalausweise automatisch gelesen werden. Die Übermittlung der Daten ist nur an Strafverfolgungsbehörden zulässig.

(2) Maßnahmen der in Absatz 1 bezeichneten Art dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Hat die Staatsanwaltschaft oder eine ihrer Ermittlungspersonen die Anordnung getroffen, so beantragt die Staatsanwaltschaft unverzüglich die richterliche Bestätigung der Anordnung. § 100b Abs. 1 Satz 3 gilt entsprechend.

(3) Die Anordnung ergeht schriftlich. Sie muß die Personen, deren Daten gespeichert werden sollen, nach bestimmten Merkmalen oder Eigenschaften so genau bezeichnen, wie dies nach der zur Zeit der Anordnung vorhandenen Kenntnis von dem oder den Tatverdächtigen möglich ist. Art und Dauer der Maßnahmen sind festzulegen. Die Anordnung ist räumlich zu begrenzen und auf höchstens drei Monate zu befristen. Eine einmalige Verlängerung um nicht mehr als drei weitere Monate ist zulässig, soweit die in Absatz 1 bezeichneten Voraussetzungen fortbestehen.

(4) Liegen die Voraussetzungen für den Erlass der Anordnung nicht mehr vor oder ist der Zweck der sich aus der Anordnung ergebenden Maßnahmen erreicht, so sind diese unverzüglich zu beenden. Die durch die Maßnahmen erlangten personenbezogenen Daten sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht oder nicht mehr benötigt werden; eine Speicherung, die die Laufzeit der Maßnahmen (Absatz 3) um mehr als drei Monate überschreitet, ist unzulässig. Ober die Löschung ist die Staatsanwaltschaft zu unterrichten."

Somit ist es nach § 3 a Abs. 2 PAuswG generell verboten, Daten in Dateien zu speichern, wenn sie durch Verwendung der Lesezone des Passes beim automatischen Lesen gewonnen wurden. Eine – und die einzige – Ausnahme stellt nach der derzeitigen Gesetzeslage die Speicherung beim Lesen aufgrund des § 163 d StPO unter den dort genannten Voraussetzungen dar, vgl. im Einzelnen Ehmann/Brunner, Pass- und Ausweisrecht, § 17 PassG, Rdnr. 11, 12; Süßmuth/Koch, Erl. zu § 3 a PAuswG, Rdnr. 26; Meyer-Goßner, StPO-Kommentar, § 163 d, Rdnr. 12.

Hieraus folgt, dass die streitbefangene Praxis nämlich das Speichern personenbezogener Daten beim automatischen Lesen des Personalausweises in Dateien, an den Pforten von Justizvollzugsanstalten, nicht erlaubt ist. Die Erfüllung der Voraussetzungen des § 163 d StPO bei dieser Führung des elektronischen Pfortenbuchs nimmt der Beklagte nicht für sich in Anspruch.

Der vom Beklagten geäußerte Standpunkt, nur den zum Abruf nach § 3 a Abs. PAuswG befugten Stellen sei die Speicherung verboten, die Vollzugsanstalten gehörten nicht zu diesen Behörden, übersieht das oben dargelegte generelle Speicherungs-Verbot. Abgesehen davon wäre es nicht nachvollziehbar, dass ein nach dieser Argumentation sogar für die in § 3 a Abs. 1 PAuswG genannten und „privilegierten" Stellen geltendes Verbot für alle sonstigen Stellen nicht gelten soll. Vor allem aber übersieht der Beklagte mit dieser Argumentation

den vom Bundesverfassungsgericht beschriebenen, oben dargelegten und in § 3 a Abs. 2 PAuswG einfachgesetzlich umgesetzten Gesetzesvorbehalt behördlicher Maßnahmen im Bereich der Einschränkung von Grundrechten, hier in der Ausprägung des Rechts auf „informationelle Selbstbestimmung". Der Vortrag des Beklagten, im Grunde geschehe mittels der elektronischen Erfassung nichts anderes als das, was bis zum Jahr 2000 in Form der handschriftlichen Eintragung der Besucherdaten in ein Pfortenbuch praktiziert und wohl auch vom Kläger als rechtmäßig angesehen worden sei, verkennt die vom Bundesverfassungsgericht in den o. g. Urteilen ausführlich dargelegten, mit der elektronischen Datenverarbeitung einhergehenden besonderen Risiken, die wegen der potentiell höheren Möglichkeit und Wahrscheinlichkeit von Grundrechtsgefährdungen erhöhte Schutzmechanismen erfordern.

Der Einwand des Beklagten, hier liege keine Speicherung „beim automatischen Lesen" i. S. d. § 3 a Abs. 2 PAuswG vor, überzeugt nicht. Soweit der Beklagte darlegt, es würden zunächst nur die in den beiden Lesezeilen im unteren Bereich der vorderen Seite des Ausweises enthaltenen Daten eingelesen, dann mittels Tastatur manuell die Adresse des Besuchers hinzugefügt, sodann die so zusammen gestellten Daten durch eine manuelle Bestätigung gespeichert und das Lesegerät diene nur als Lese- und Eingabehilfe, muss er sich Folgendes entgegenhalten lassen.

Trotz der Tatsache, dass außer der durch das Lesegerät automatisch gelesenen Datenmenge A noch eine durch das Auge des Bediensteten gelesene und von Hand eingegebene Datenmenge B hinzugefügt und die nunmehr Gesamtmenge A+B in einer Datei, dem elektronischen Pfortenbuch, gespeichert wird, bleibt es bei dem folgenden Tatbestand: Die durch das Lesegerät automatisch gelesene Datenmenge A wird gespeichert. Dadurch, dass die JVA das Lesegerät als „Lese- und Eingabehilfe" benutzt und das Gelesene dann speichert, werden die vom Bundesverfassungsgericht beschworenen Gefahren der elektronischen Datenverarbeitung potentiell akut und wird das datenschutzrechtliche Sicherungsbedürfnis ausgelöst.

Der Vortrag, dass das Lesen und das Speichern nicht exakt gleichzeitig geschehe, sondern zeitlich erst nach dem manuellen Erfassen der Datenmenge B und einem Speicherbefehl erfolge, ist nicht geeignet, Zweifel am Vorliegen der Speicherung beim Lesen zu wecken. Entscheidend ist, dass es sich um einen einheitlichen Ablauf handelt, der von Anfang an dem Ziel folgt, die Datenmenge A sogleich zu speichern.

Die Notwendigkeit eines Speicherbefehls kann den Ablauf-Zusammenhang nicht zerstören. Er wird sogar in aller Regel selbstverständlicher Bestandteil eines Speicherungsvorgangs sein. Wegen der vom Beginn des Ablaufs in Gestalt des automatischen Lesens bereits gegebenen Zielgerichtetheit auf das Speichern hin stört auch die im selben Arbeitsgang vorgenommene, wenige Sekunden beanspruchende Eingabe der Datenmenge B den Zusammenhang nicht. Am Schluss dieses einheitlichen Ablaufs steht der Speicherbefehl, der sich auf beide Datenmengen bezieht. Die Landesbeauftragte für den Datenschutz und Informationsfreiheit hat in ihrem 16. Datenschutzbericht, S. 165, 166, zu Recht angeführt, das Gesetz meine mit Speichern „beim automatischen Lesen" nicht lediglich ein technisch gleichzeitig erfolgendes Einlesen und Speichern. Es komme nicht auf die technische, auf Sekundenbruchteile exakte Gleichzeitigkeit von Lesen und Speichern an. Dies stimmt auch unter dem Gesichtspunkt, dass man, die Lesart des Beklagten als richtig unterstellt, durch zeitliches Abwarten des Speicherns oder die beliebig gestaltbare Zwischenschaltung von Befehlen, das Gesetz mit Leichtigkeit umgehen könnte.

Die Frage, ob – wie der Kläger meint – ohnehin bereits das Speichern des Leseergebnisses beim Lesevorgang im Arbeitsspeicher eine Speicherung i. S. d. § 3 a Abs. 2 PAuswG darstellt, kann daher offen bleiben. Die Kammer merkt aber Folgendes an. Gemäß § 3 Abs. 2 Nr. 2 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW), fast wortgleich mit § 3 Abs. 4 Nr. 1 Bundesdatenschutzgesetz (BDSG), ist Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung.

Grundsätzlich mag auch das Festhalten von Daten in einer Zwischendatei Speicherung im datenschutzrechtlichen Sinn sein können, so Bergmann/Möhrle/Herb, Datenschutzrecht, Stand: Januar 2008, § 3, Rdnr. 81.

Entscheidend bzw. erforderlich ist dabei aber in jedem Fall, dass die Information nach dem Fixieren auf einem Datenträger wiedergewonnen werden kann, Stähler, Kommentar zum DSG NRW, E, Erl. zu § 3, Rdnr. 11, sie also für eine spätere Wahrnehmung „nachlesbar" festgehalten wird, Gola/Schomerus, BDSG-Kommentar, 9. Auflage, § 3 Rdnr. 26, 27.

Dies wird bei einem reinen Arbeitsspeicher jedenfalls dann nicht der Fall sein, wenn die temporal abgelegten Informationen nicht wenigstens durch Einzeleingabe oder eine besondere Programmierung unter einer speziellen, die Rückholbarkeit gewährleistenden Zwischendatei-Bezeichnung – und sei es automatisch – in einem besonderen temporären Verzeichnis gesichert, sondern lediglich unbenannt bis zu ihrer Überschreibung vorhanden bleiben. Eine Zwischendatei-Sicherung müsste überdies zum Zweck ihrer weiteren Verarbeitung, also zum Zweck des Rückgriffs, erfolgen.

Der Klageantrag zu 2., die anlässlich des (weiteren) Besuchs des Klägers vom 6. Februar 2003 in der Justizvollzugsanstalt Aachen gespeicherten Daten

zu löschen, ist ebenfalls begründet. Gemäß § 19 Abs. 3 a) DSG NRW sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Dies ist hier wegen des Verstoßes gegen das Speicherungsverbot in § 3 a Abs. 2 PAuswG der Fall.