

Rechtsprechung der niedersächsischen Justiz

Datenschutzrechtliches Verbot des Scannens von Personalausweisen

1. Soweit die Erhebung und Verwendung personenbezogener Daten aus dem Personalausweis oder mithilfe des Personalausweises betroffen ist, enthalten die Vorschriften des dritten Abschnitts des Personalausweisgesetzes eine abschließende, § 28 BDSG verdrängende Regelung.

2. Das Scannen und Speichern von Personalausweisen durch nicht öffentliche Stellen ist nach den datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes unzulässig.

VG Hannover 10. Kammer, Urteil vom 28.11.2013, 10 A 5342/11

§ 1 Abs 3 S 1 BDSG, § 28 BDSG, § 3 BDSG, § 38 Abs 5 BDSG, § 38 Abs 6 BDSG, § 14 PAuswG, § 20 PAuswG

Tenor

Die Klage wird abgewiesen.

Die Klägerin trägt die Kosten des Verfahrens; insoweit ist das Urteil vorläufig vollstreckbar.

Tatbestand

- 1 Die Beteiligten streiten um die Rechtmäßigkeit einer datenschutzrechtlichen Anordnung des Beklagten.
- 2 Die Klägerin ist eine Logistikdienstleisterin, die insbesondere im Bereich der Automobillogistik und Autotransporte tätig ist. Auf ihrem Betriebsgelände lagern ständig mehrere tausend Fahrzeuge. Täglich werden zahlreiche Fahrzeuge - insbesondere von Fahrern von Speditionen - abgeholt. Um den Speditionsvorgang zu überwachen, werden die Personalausweise der Abholer eingescannt und auf einem Rechner gespeichert.
- 3 Nachdem der Beklagte durch mehrere Eingaben von Betroffenen Kenntnis von dieser Praxis erhalten hatte, wandte er sich im Juli 2011 an die Klägerin, teilte ihr mit, dass er das Einscannen von Personalausweisen für unzulässig halte und bat um Stellungnahme. Hierauf äußerte die Klägerin gegenüber dem Beklagten, die von ihr geübte Praxis sei mit den datenschutzrechtlichen Bestimmungen vereinbar. Die eingescannten Personalausweise der Abholer würden auf einem gesonderten Rechner gespeichert und gelöscht, sobald eine positive Rückmeldung über die Fahrzeugauslieferung vorliege; in der Regel sei dies nach spätestens fünf Tagen der Fall. Das Wachgebäude, in dem sich der Rechner befinde, sei während der Geschäftszeiten ständig besetzt und werde auch ansonsten überwacht; unbefugte Dritte könnten sich daher die Daten nicht zugänglich machen. Nach § 28 Abs. 1 Nr. 2 des Bundesdatenschutzgesetzes (BDSG) sei das Erheben, Speichern und Nutzen von personenbezogenen Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich sei und kein Grund zu der Annahme bestehe, dass ein schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiege. Unter Berücksichtigung der hohen Werte, die den Spediteuren oder Fahrern übergeben würden, könne ein berechtigtes Interesse an der Datenerhebung, die gerade dazu diene, den reibungslosen Speditionsvorgang zu überwachen und gegebenenfalls einen Ansprechpartner zu haben, nicht ernstlich in Zweifel gezogen werden. Vorwiegend komme es in diesem Zusammenhang zwar auf den Namen und die Adresse der Fahrzeugabholer an, aber auch das Lichtbild und die weiteren Informationen zum Erscheinungsbild wie Körpergröße und Augenfarbe könnten insbesondere im Falle einer Straftat der Erleichterung der polizeilichen Ermittlungen dienen. Überwiegende schutzwürdige Interessen der Betroffenen seien nicht ersichtlich. Werde der Speditionsvorgang erfolgreich abgeschlossen, würden die Daten nicht anderweitig genutzt, sondern gelöscht.
- 4 Mit Bescheid vom 07.11.2011 gab der Beklagte der Klägerin unter Androhung eines Zwangsgeldes für den Fall der Nichtbefolgung auf, innerhalb von einer Woche nach Bestandskraft der Anordnung das Einscannen von Personalausweisen zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen: Die Voraussetzungen des § 28 BDSG lägen nicht vor. Zu Unrecht berufe sich die Klägerin darauf, die von ihr erhobenen Daten dienten insbesondere im Falle einer Straftat der Erleichterung der polizeilichen Ermittlungen. Da die Ermittlungsbehörden die Daten wie Lichtbild, Körpergröße, Augenfarbe usw. bei den Meldebehörden abrufen könnten, sei die Erhebung durch die Klägerin nicht erforderlich und damit unzulässig. Darüber hinaus sei nach dem Personalausweisgesetz das Scannen von Ausweisdaten untersagt. Der Ausweis dürfe lediglich als Identitätsnachweis und Legitimationspapier verwendet, d.h. zur Einsichtnahme vorgelegt werden.

- 5 Zur Begründung ihrer am 08.12.2011 erhobenen Klage wiederholt die Klägerin unter Vertiefung im Einzelnen ihr Vorbringen aus dem Verwaltungsverfahren. Aus Zeitgründen sei es gerechtfertigt, eine Kopie der Personalausweise anzufertigen. Die eingescannten Unterlagen dienten der Ermittlung von Straftätern; dem von ihr praktizierten Verfahren komme zugleich eine präventive Wirkung zu. Sobald der jeweilige Speditionsvorgang abgeschlossen sei - in der Regel spätestens nach 5 Tagen -, würden die Daten wieder gelöscht.
- 6 Die Klägerin beantragt,
- 7 die Untersagungs- und Anordnungsverfügung des Beklagten vom 07.11.2011 aufzuheben.
- 8 Der Beklagte beantragt,
- 9 die Klage abzuweisen.
- 10 Er beruft sich auf die Begründung des angefochtenen Bescheides und macht ergänzend geltend, zur Wahrung der berechtigten Interessen der Klägerin sei es ausreichend, wenn sich ihre Mitarbeiter den Personalausweis des jeweiligen Abholers zeigen ließen und zu Identifikationszwecken den Namen, die Adresse und das Geburtsdatum notieren würden.
- 11 Wegen des weiteren Vorbringens der Beteiligten und der Einzelheiten des Sachverhalts wird auf den Inhalt der Gerichtsakten und der beigezogenen Verwaltungsvorgänge Bezug genommen. Sämtliche Akten waren Gegenstand der mündlichen Verhandlung.

Entscheidungsgründe

- 12 Die zulässige Klage ist nicht begründet.
- 13 Der angefochtene Bescheid ist rechtmäßig und verletzt die Klägerin daher nicht in ihren Rechten (vgl. § 113 Abs. 1 Satz 1 VwGO).
- 14 Rechtsgrundlage für die vom Beklagten getroffenen Anordnungen ist § 38 Abs. 5 Satz 2 BDSG. Nach § 38 Abs. 5 Satz 1 BDSG kann die Aufsichtsbehörde zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz gegenüber nicht-öffentlichen Stellen Maßnahmen u.a. zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten anordnen. Gemäß § 38 Abs. 5 Satz 2 BDSG kann sie bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Die Anordnung des Beklagten, das Verfahren „Einscannen von Personalausweisen“ einzustellen und die bisher rechtswidrig erhobenen Daten zu löschen, stellt eine Maßnahme im Sinne der letztgenannten Vorschrift dar.
- 15 Der Beklagte ist für den Erlass des streitbefangenen Bescheides zuständig. Gemäß § 38 Abs. 6 BDSG bestimmen die Landesregierungen oder die von ihnen ermächtigten Stellen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich des dritten Abschnitts des Bundesdatenschutzgesetzes zuständigen Stellen. Die Vorschriften des dritten Abschnitts finden u.a. Anwendung, soweit durch nicht-öffentliche Stellen personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten von solchen Stellen in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden (§ 27 Abs. 1 Satz 1 BDSG). Die Klägerin als juristische Person des Privatrechts ist gemäß § 2 Abs. 4 Satz 1 BDSG eine nicht-öffentliche Stelle im vorbenannten Sinne, so dass für ihre Kontrolle der von der Niedersächsischen Landesregierung durch Beschluss vom 19.12.2006 (Nds. MBl. 2007, 108) als zuständige Aufsichtsbehörde nach § 38 Abs. 6 BDSG bestimmte Beklagte zuständig ist. Die örtliche Zuständigkeit des Beklagten folgt aus § 1 Abs. 1 Nds. VwVfG, § 3 Abs. 1 Nr. 2 VwVfG. Auch ansonsten sind formelle Mängel nicht erkennbar, insbesondere ist die Klägerin vor Erlass der angefochtenen Verfügung in einer § 1 Abs. 1 Nds. VwVfG, § 28 Abs. 1 VwVfG entsprechenden Weise angehört worden.
- 16 Die von dem Beklagten angeordneten Maßnahmen sind auch inhaltlich nicht zu beanstanden. Das von der Klägerin praktizierte Scannen und Speichern von Personalausweisen stellt einen schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften dar, so dass es der Beklagte auf der Grundlage von § 38 Abs. 5 Satz 2 BDSG verbieten und die Löschung der bisher rechtswidrig erhobenen Daten anordnen kann.
- 17 Die Zulässigkeit des Scannens und Speicherns von Personalausweisen beurteilt sich nach den in Abschnitt 3 des Gesetzes über Personalausweise und den elektronischen Identitätsnachweis - Personalausweisgesetz - (PAuswG) getroffenen Regelungen über den Umgang mit personenbezogenen Daten; die von den Beteiligten herangezogene Vorschrift des § 28 BDSG über die Datenerhebung und -speicherung für eigene Geschäftszwecke durch nicht-öffentliche Stellen ist hingegen nicht anwendbar.
- 18 Nach § 1 Abs. 2 Nr. 3 BDSG gilt das Bundesdatenschutzgesetz zwar grundsätzlich auch für die Datenerhebung, -nutzung und -verarbeitung durch nicht-öffentliche Stellen. Soweit aber andere

Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften des Bundesdatenschutzgesetzes vor (§ 1 Abs. 3 Satz 1 BDSG). Die Konkurrenz von Rechtsvorschriften des Bundes innerhalb und außerhalb des Bundesdatenschutzgesetzes, deren Gegenstand die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist, wird durch diese Regelung im Sinne des Vorrangs der spezielleren - bereichsspezifischen - Norm geklärt (vgl. Dix in Simitis, Bundesdatenschutzgesetz, 7. Aufl., Rn. 158 zu § 1). Inwieweit sich der Vorranggrundsatz konkret auswirkt, bestimmt sich nach dem Inhalt der mit dem Bundesdatenschutzgesetz konkurrierenden Vorschrift. Soweit diese eine abweichende Regelung für einen Sachverhalt trifft, der ebenfalls im Bundesdatenschutzgesetz geregelt ist, verdrängt sie die Normen dieses Gesetzes.

- 19 Soweit es um die Erhebung und Verwendung personenbezogener Daten aus dem Personalausweis oder mithilfe des Personalausweises geht, enthalten die Vorschriften des dritten Abschnitts des Personalausweisgesetzes eine abschließende, § 28 BDSG verdrängende Regelung. Denn § 14 PAuswG mit der amtlichen Überschrift „Erhebung und Verwendung personenbezogener Daten“ bestimmt, dass die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises ausschließlich erfolgen darf durch
 - 20 1. zur Identitätsfeststellung berechnigte Personen nach Maßgabe der §§ 15 bis 17,
 - 21 2. öffentliche Stellen und nicht-öffentliche Stellen nach Maßgabe der §§ 18 bis 20.
- 22 Damit ist diese Norm die zentrale bereichsspezifische Datenschutzvorschrift des Personalausweisrechts (so Möller in Hornung/Möller, PassG - PAuswG, Kommentar 2011, Rn. 1 zu § 14), die keinen Raum für eine vorrangige oder auch nur ergänzende Heranziehung der Regelungen des dritten Abschnitts des Bundesdatenschutzgesetzes über die Datenverarbeitung nicht-öffentlicher Stellen lässt.
- 23 Die Klägerin ist unstrittig keine zur Identitätsfeststellung berechnigte Behörde im Sinne von § 14 Nr. 1 PAuswG. Maßgeblich für die Zulässigkeit des beanstandeten Verfahrens ist daher § 20 PAuswG. Absatz 1 dieser Norm bestimmt, dass der Inhaber den Personalausweis bei öffentlichen und nicht-öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden kann und ist damit die Grundlage für die Verwendung als Ausweis und Legitimationspapier auch im privaten Rechtsverkehr (Möller in Hornung/Möller, PassG - PAuswG, Kommentar 2011, Rn. 3 zu § 20). Dem entsprechend gesteht der Beklagte der Klägerin auch ohne weiteres zu, dass sie sich von den Fahrzeuge abholenden Personen den Personalausweis zeigen lässt und darin enthaltene Daten (Namen, Geburtsdatum, Adresse) heraus schreibt.
- 24 Das mit der angefochtenen Verfügung beanstandete Verfahren hingegen ist § 20 Abs. 2 PAuswG zuzuordnen, wonach außer zum elektronischen Identitätsnachweis der Personalausweis durch öffentliche oder nicht-öffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden darf. Nach der zur Konkretisierung der datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes heranzuziehenden Begriffsbestimmung in § 3 Abs. 2 Satz 1 BDSG (vgl. BT-Drs. 16/10489 S. 40 zu § 14) ist eine automatisierte Verarbeitung die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen, wobei zum Verarbeiten das Speichern von personenbezogenen Daten gehört (§ 3 Abs. 4 Satz 1 BDSG). Ungeachtet der dabei angewendeten Verfahren ist Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Angesichts dieses Regelungsgefüges kann es nicht ernsthaft zweifelhaft sein, dass das von der Klägerin praktizierte Verfahren, bei dem Personalausweise gescannt und unter Verwendung einer speziellen Software auf einem Rechner gespeichert werden, um im Bedarfsfall verwendet zu werden, als automatisierte Speicherung personenbezogener Daten im Sinne von § 20 Abs. 2 PAuswG zu qualifizieren ist; auch die Klägerin hat substantiierte Einwände insoweit nicht erhoben.
- 25 Dieses Ergebnis wird durch die Entstehungsgeschichte von §§ 14 und 20 PAuswG bestätigt. So heißt es in der Begründung des Regierungsentwurfs zu § 14, der unverändert Gesetz geworden ist, u.a. (BT-Drs. 16/10498 S. 40):
- 26 „§ 14 stellt klar, dass die Erhebung und Verwendung personenbezogener Daten aus oder mithilfe des Ausweises künftig nur über die dafür vorgesehenen Wege erfolgen darf. Dies sind für nichtöffentliche und öffentliche Stellen der elektronische Identitätsnachweis und für zur hoheitlichen Identitätsfeststellung berechnigte Behörden der Abruf der elektronisch gespeicherten Daten einschließlich der biometrischen Daten. Weitere Verfahren z.B. über die optoelektronische Erfassung („scannen“) von Ausweisdaten oder den maschinenlesbaren Bereich sollen ausdrücklich ausgeschlossen werden.“
- 27 Dem entsprechend wird in der Begründung zu § 20 Absätze 2 und 3, der ebenfalls im Gesetzgebungsverfahren nicht verändert wurde, ausgeführt (BT-Drs. 16/10498 S. 42):
- 28 „Die Vorschrift ist erforderlich, weil der Einsatz des elektronischen Identitätsnachweises sowohl zu einem automatischen Abruf von Daten (z.B. bei der erneuten Anmeldung bei einem Dienstkonto) als auch zur automatischen Speicherung personenbezogener Daten (z.B. nach Übermittlung von Daten zur Anlage eines Dienstkontos) führen kann. Jenseits dieser engen Ausnahmen - die der Ausweisinhaber über die Eingabe seiner Geheimnummer steuern kann - bleiben die

Verwendungsverbote der bisherigen Fassung von § 3 Abs. 4 Satz 1 PersAuswG und § 16 Abs. 4 Satz 1 PassG, § 3a Abs. 1 Satz 1 und Abs. 2 erster Halbsatz und § 4 Abs. 2 und 3 des Personalausweisgesetzes erhalten. Von der Vorschrift erfasst sind alle Formen des automatischen Abrufs, insbesondere Scannen, Fotokopieren und Ablichten der Daten. ..."

- 29 Ob tatsächlich schon das bloße Kopieren von Personalausweisen - von ausdrücklich gesetzlich zugelassenen Ausnahmen wie in § 8 Abs. 1 Satz 3 Geldwäschegesetz, § 95 Abs. 4 Satz 2 Telekommunikationsgesetz und § 64 Abs. 1 Nr. 2 Fahrerlaubnisverordnung abgesehen - nach Wortlaut sowie Sinn und Zweck der datenschutzrechtlichen Vorschriften des Personalausweisgesetzes verboten ist, bedarf hier keiner Entscheidung, da das von der angefochtenen Verfügung erfasste Scannen und automatisierte Speichern mit der Möglichkeit der Weiterverarbeitung und Nutzung eine andere rechtliche Qualität aufweist. Lediglich vorsorglich ist deshalb darauf hinzuweisen, dass nach dem vom Beklagten vorgelegten Schreiben des Bundesministeriums des Innern an den Bundesbeauftragten für den Datenschutz vom 01.02.2013 zwar kein grundsätzliches rechtliches Kopierverbot (mehr) besteht, für das Anfertigen von Kopien des Personalausweises (bzw. des Reisepasses) aus sicherheits- und datenschutzrechtlichen Gründen jedoch strenge Maßstäbe gelten sollen. Bei einer Identifizierung unter Anwesenden sei die Erstellung einer Kopie grundsätzlich unzulässig, weil regelmäßig kein Bedarf dafür bestehe.
- 30 Ohne Einfluss auf die rechtliche Zulässigkeit des von der Klägerin praktizierten Verfahrens ist die Frage, ob im Einzelfall eine wirksame Einwilligung des Personalausweisinhabers vorliegt. Das Scannen und Speichern von Personalausweisen ist nach den zuvor dargestellten Normen gesetzlich verboten, ohne dass dem Ausweisinhaber die Möglichkeit eingeräumt worden wäre, das Verbot durch sein Einverständnis zu suspendieren. Eine die Erhebung, Verarbeitung und Nutzung personenbezogener Daten rechtfertigende Einwilligung des Betroffenen, wie sie in § 4 Abs. 1, § 4a BDSG geregelt ist, sieht das Personalausweisgesetz als hier einschlägige Spezialvorschrift nicht vor.
- 31 Das von der Klägerin praktizierte Verfahren des Scannens und Speicherns von Personalausweisen stellt einen schwerwiegenden Verstoß gegen die datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes dar, so dass der Beklagte hiergegen auf der Grundlage von § 38 Abs. 5 Satz 2 BDSG einschreiten kann. Grundsätzlich setzt eine Untersagung nach dieser Vorschrift zwar voraus, dass zuvor nach § 38 Abs. 5 Satz 1 BDSG vergeblich die Beseitigung des Mangels verlangt wurde und auch die Festsetzung eines Zwangsgeldes nicht zum Erfolg geführt hat. Steht jedoch die Unmöglichkeit der Fehlerbeseitigung von vornherein fest, kann ausnahmsweise unmittelbar das Datenverarbeitungsverfahren untersagt werden (Petri in Simitis, Bundesdatenschutzgesetz, 7. Aufl., Rn. 75 zu § 38). So verhält es sich hier, da eine Legalisierung des von der Klägerin praktizierten Verfahrens durch bloße Modifikationen nicht möglich ist.
- 32 Als Unterlegene hat die Klägerin gemäß § 154 Abs. 1 VwGO die Kosten des Verfahrens zu tragen. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 167 VwGO in Verbindung mit § 708 Nr. 11 ZPO.