

„Mittelfristig geht kein Weg an einer umfassenden Verfahrensrevision vorbei“

Interview mit Thilo Weichert



Das elektronische Lastschriftverfahren hatte der Gesetzgeber bei der Novelle des Bundesdatenschutzgesetzes nicht im Blick. So erklärt Thilo Weichert die Tatsache, dass sich dessen Praxis kaum mit den datenschutzrechtlichen Anforderungen vereinbaren lässt. Entscheidend für den rechtlich zulässigen Fortbestand des Verfahrens ist seiner Einschätzung nach die Änderung des Einwilligungsverfahrens. Die Zustimmung des Kunden dürfe künftig nicht mehr erst an der Kasse eingeholt werden. Scoringbasierte Verfahren der Bonitätsprüfung sollten die Netzbetreiber am besten sofort einstellen. Generell empfiehlt Weichert der Branche, vorsichtshalber alle elektronischen Zahlverfahren auf ihre datenschutzrechtliche Zulässigkeit abzuklopfen. Red.

Karten Wie kommt es, dass das elektronische Lastschriftverfahren gerade jetzt und nicht schon früher ins Visier der Datenschützer geraten ist? Ist es erst durch die Novelle des Bundesdatenschutzgesetzes problematisch geworden? Oder war es das schon immer?

Die Thematisierung erfolgte primär nicht durch die Datenschutzaufsichtsbehörden, sondern durch die Medien, die besonde-

re Auswüchse problematisierten. Daraufhin mussten wir Aufsichtsbehörden reagieren und prüfen. Dabei stellten wir fest, dass sich das ELV von vor mehreren Jahren – von uns unbemerkt – derart weiterentwickelt hat, dass die Praktiken weder gesetzeskonform sind noch so noch akzeptiert werden können.

Die BDSG-Novelle hat damit nichts direkt zu tun, außer, dass der Gesetzgeber offensichtlich, wohl durch die Datenschutzskandale seit 2008, sensibler geworden ist hinsichtlich des Umgangs mit Finanztransaktionsdaten. Dass der Gesetzgeber dann ein Gesetz gemacht hat, das mit den ELV-Bonitätsprüfungen nicht ansatzweise in Einklang zu bringen



Dr. Thilo Weichert, Leiter des Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein, Kiel

ist, liegt daran, dass er diesen Anwendungsfall überhaupt nicht im Blick hatte.

Karten Was sind unter Datenschutz-Gesichtspunkten die Hauptkritikpunkte am elektronischen Lastschriftverfahren?

Wir haben viele Kritikpunkte. Die eingeholten Einwilligungen sind weder informiert noch freiwillig und erfolgen zeitlich zu spät. Es mangelt an jeglicher Transparenz; die Betroffenen haben keine Ahnung, was sich da im Hintergrund mit ihren Daten alles abspielt. Dies gilt vor allem für das ausgeklügelte Verfahren der Bonitätsprüfungen, des Führens von sogenannten White und Black Lists und die dabei praktizierten Scoringberechnungen.

Was absolut illegal ist, ist die Nutzung dieser Daten für Zwecke der Werbung oder der Kundenbindung, so wie dies im Fall von Easycash bekannt geworden ist.

Karten Muss sich der Handel auf das Ende von ELV einrichten? Oder ist aus Ihrer Sicht ein datenschutzrechtlich sauberes ELV denkbar?

Die Diskussionen zwischen Aufsichtsbehörden und Unternehmensvertretern sind

noch nicht am Ziel. Es gibt zweifellos in einzelnen Aspekten auch unterschiedliche Meinungen bei uns Datenschützern. Grundsätzlich ist ELV natürlich möglich, wenn ein sauberes Einwilligungsverfahren praktiziert wird. Das hinzubekommen ist aber angesichts der Situation an der Kasse, die keine umfassende Information und keine Bedenkzeit zulässt, nicht gerade trivial.

Karten Was müsste dafür am Verfahren geändert werden?

Wie gesagt, wir sind hier mit den Diskussionen noch nicht am Ende. Reale Information und reale Wahlfreiheit sind aber unabdingbar. Es ist ein Unding, dass ein Kunde nur seine Karte hingibt und dann keine weitere Möglichkeit mehr hat, den Lauf seiner Daten zu verfolgen.

Ich denke, eine Lösung könnte darin bestehen, dass die Betroffenen nicht an der Kasse, sondern zu einem früheren Zeitpunkt ein möglichst unabhängig zertifiziertes Verfahren konsentieren.

Das Bundesverfassungsgericht spricht vom Grundrecht auf informationelle Selbstbestimmung. Dies setzt Wissen und Wollen voraus. Davon kann beim Elektronischen Lastschriftverfahren derzeit nicht die Rede sein.

Karten Kommen hier die Emittenten ins Spiel, etwa indem der Kunde

Beilagenhinweis

Dieser Ausgabe liegt das Sachregister 2010 von **cards Karten cartes** bei.

gleich bei Beantragung der Karte darüber entscheidet, ob er mit der Nutzung der Daten fürs Lastschriftverfahren einverstanden ist oder nicht? Oder müsste das jeder Händler selbst organisieren?

Das könnte eine Lösung sein. Die setzt aber voraus, dass einheitliche Verfahren verabredet und praktiziert werden. Möglich wäre dies eventuell über Verhaltensregeln nach § 38 a BDSG. Realistischer ist wohl, entweder beim Händler oder beim Dienstleister anzusetzen.

Karten Lässt sich eine Bonitätsprüfung, wie sie heute dargestellt wird, überhaupt datenschutzkonform gestalten? Oder müsste der Handel darauf in jedem Fall verzichten?

Bonitätsprüfungen waren schon immer heikel. Sie sind aber auch schon immer grundsätzlich zulässig. Das hat der Gesetzgeber 2009 mit seinen Regelungen zum Scoring und zu Auskunftfeien erneut eindeutig zum Ausdruck gebracht. Dabei hatte er aber die klassische Kreditgewährung vor Augen, nicht die beiläufige Vorausfinanzierung von zumeist Kleinbeträgen.

Knüpfen Bonitätsprüfungen an gesicherten Daten zum Betroffenen selbst an, so ist das im Grundsatz in Ordnung. Kuno und objektivierte Sperrlisten sind nicht das Problem. Heikel sind dagegen generell Scoringverfahren, bei denen spekuliert wird, bei denen mit statistischen (Vor-) Urteilen gearbeitet wird und bei denen keine Kontrollmöglichkeiten für die Betroffenen bestehen.

Karten Wie sollen Netzbetreiber sich jetzt verhalten?

Ich könnte es mir natürlich einfach machen und sagen: sich rechtskonform verhalten. Dafür sind die Finanzdienstleister selbst verantwortlich. Natürlich wollen wir Aufsichtsbehörden dabei helfen, wenn tatsächlich die Bereitschaft zur Annahme von Hilfe besteht. So, wie wir bisher teilweise an der Nase herumgeführt wurden, kann man dies jedoch bezweifeln.

Kurzfristig werden wir nur solche Verfahren beanstanden, denen die Rechtswidrigkeit auf der Stirn steht. Aber mittelfristig geht kein Weg an einer umfassenden Verfahrensrevision vorbei.

Karten Empfehlen Sie Sofortmaßnahmen, um rechtlich auf der sicheren Seite zu sein?

Meines Erachtens rechtlich heute einfach machbar wäre die Abwicklung des Elektronischen Lastschriftverfahrens durch die Dienstleister als Auftragnehmer. Dies hätte aber zur Folge, dass Sperrlisten und Positivempfehlungen nur jeweils für den einzelnen Auftraggeber, also den Händler, geführt werden dürften.

Karten Wie ist das PIN-gestützte Girocard-Verfahren datenschutzrechtlich zu bewerten?

Nach den Erfahrungen mit dem ELV werde ich nicht den Fehler begehen und einen Blankoscheck ausstellen. Eine abschließende Bewertung setzt eine umfassende Bestandsaufnahme voraus. Dazu sind wir Aufsichtsbehörden mit unseren begrenzten Ressourcen überhaupt nicht in der Lage. Das ist auch Aufgabe der Branche selbst.

„Rechtlich heute machbar wäre die Abwicklung des ELV durch die Dienstleister als Auftragnehmer.“

„Eine Lösung könnte darin bestehen, dass die Betroffenen zu einem früheren Zeitpunkt ein Verfahren konsentieren.“

„Bei Girocard sehe ich nicht die großen Probleme wie beim ELV.“

Dennoch: Da hier ein direktes Zahlungsverfahren stattfindet und alle Datenflüsse zweckgebunden bleiben dürften, sehe ich nicht die großen Probleme wie beim ELV.

Karten Und wie sieht es mit Kreditkartenzahlungen aus?

Auch hier basiert die Betrugserkennung schließlich auf der Analyse von Transaktionsmustern auf Basis der gesammelten Daten ...

Das zum ec-PIN-Verfahren Gesagte gilt generell auch für Kreditkarten. Hinsichtlich der Betrugserkennung muss hier genau darauf geachtet werden, dass Warn- und Sperrfunktionen objektiv sind und transparent ablaufen. Das Unabhängige Landeszentrum für Datenschutz in Kiel hat ein Verfahren zur Risikobewertung datenschutzrechtlich zertifiziert, das mit Datenaggregation und Pseudonymisierung arbeitet. Bei Bonitätsprüfungen muss eben nicht nur die Effektivität aus Sicht des Finanzdienstleisters beachtet werden; die betroffenen Menschen und deren Rechte müssen von Anfang an hinreichend berücksichtigt werden.

Karten Allzu viel Transparenz hat sich im Ausland aber nicht bewährt. So hat die Offengung von Prinzipien, mit denen die Betrugserkennungs-Systeme arbeiten, dafür gesorgt, dass eben diese Merkmale umgangen wurden. Wie lässt sich dieser Konflikt zwischen Transparenz und Effektivität der Systeme lösen? Schließlich ist eine wirkungsvolle Betrugsabwehr auch im Sinne der Kunden.

Die Diskussion über die Offenlegung von Datenauswertungen wird auch beim Creditscoring geführt. Dort wie hier gilt: Objektive Kriterien lassen sich nicht oder nur schwer manipulieren. Bei spekulativen Systemen ist dies wohl anders, diese haben aber auch ein hohes Diskriminie-

rungspotenzial. Es geht nicht darum, Betrugserkennungssysteme bis in den Sourcecode hinein offenzulegen.

„Es geht nicht darum, Betrugserkennungssysteme bis in den Sourcecode hinein offenzulegen.“

Wohl aber geht es bei unserer Transparenzforderung darum, Betroffenen die Möglichkeit zu geben, sich gegen im Einzelfall unberechtigte statistische Vorurteile erfolgreich zur Wehr setzen zu können.

Karten Gibt es überhaupt elektronische Zahlverfahren, die sich als datenschutzrechtlich unbedenklich bezeichnen lassen? Oder gehört jetzt alles auf den Prüfstand?

Natürlich gibt es datenschutzkonforme elektronische Zahlverfahren. Gegen anonyme Prepaid-Karten ist zum Beispiel überhaupt nichts einzuwenden. Das Problem ist der unkontrollierte Wildwuchs.

Insofern würde ich es sehr begrüßen, wenn wirklich mal alles auf den Prüfstand gestellt würde.

Dies sollte nicht repressiv von uns Datenschützern ausgehen. Die Payment-Branche kann das selbst anstoßen, indem sie ihre Verfahren evaluieren oder noch besser transparent und unabhängig zertifizieren lässt. Vielleicht bekommen wir mit der Stiftung Datenschutz hierfür bald einen zuverlässigen institutionellen Rahmen.