

## Begründung der Beanstandung

### Verlust eines USB-Sticks mit Daten aller Elektronischen Grundbücher der Amtsgerichtsbezirke Demmin und Ribnitz-Damgarten; Beanstandung gemäß § 32 Landesdatenschutzgesetz

Im Zusammenhang mit dem Verlust eines USB-Sticks, der ca. 9GB Daten aller Elektronischen Grundbücher der Amtsgerichtsbezirke Demmin und Ribnitz-Damgarten (ca. 34 000 Grundbücher) in unverschlüsselter Form enthielt, **beanstande** ich gemäß § 32 Landesdatenschutzgesetz (DSG M-V):

1. Verstöße gegen die Pflichten des Justizministeriums als Auftraggeber bei der Verarbeitung personenbezogener Daten gem. § 4 DSG M-V,
2. Verstöße gegen die Pflicht zur Gewährleistung der Vertraulichkeit durch technische und organisatorische Maßnahmen gem. § 21 Abs. 2 Nr. 1 DSG M-V.

#### A) Dieser Beanstandung liegt folgender **Sachverhalt** zugrunde:

Zwischen dem 6. und 9. März 2009 ist in den Räumen der vom Justizministerium mit dem technischen Betrieb der Elektronischen Grundbücher in Mecklenburg-Vorpommern beauftragten Fa. D. ein USB-Stick mit Kopien der Echt Datenbanken aller Elektronischen Grundbücher der Grundbuchämter Demmin und Ribnitz-Damgarten abhanden gekommen. Diese enthielten die Angaben aus ca. 34.000 Grundbüchern und sollten für Zwecke der Wartung und Störungsbeseitigung einem weiteren Auftragnehmer, der Fa. R., übergeben werden.

Zur Bereitstellung der Daten wurde bis zu dem genannten Zeitpunkt folgendes Verfahren angewendet: Jeder Datenbankexport zur Fehleranalyse bei der Fa. R. bedurfte einer ausdrücklichen Anforderung durch das Justizministerium. Lag diese vor, wurde zunächst auf den Systemen der Fa. D. eine Kopie der Datenbanken im Export-Format des verwendeten Datenbank-Systems hergestellt. Diese Kopien wurden sodann mit einem handelsüblichen Programm komprimiert und auf einem USB-Stick gespeichert. Dieser sollte Fa. R. zur Wartung und zur Störungsbeseitigung übergeben werden.

Da sich im vorliegenden Fall die Übergabe des USB-Sticks von einem Freitag auf den folgenden Montag verzögerte, wurde dieser durch den verantwortlichen Mitarbeiter nicht ordnungsgemäß verschlossen, sondern offen auf dem Schreibtisch liegen gelassen. Bei Dienstantritt am darauffolgenden Montag konnte der USB-Stick trotz umfangreicher Suchmaßnahmen nicht mehr aufgefunden werden. Sowohl eine Befragung der zugangsberechtigten Mitarbeiter als auch des Reinigungspersonals durch die Fa. D., als auch durch die von ihr verständigte Staatsanwaltschaft blieb ohne Erfolg. Das gegen Unbekannt eingeleitete Ermittlungsverfahren ist am 27. Juli 2009 wegen fehlender Ermittlungsansätze eingestellt worden.

Das Justizministerium hat mich am 12. März 2009 erstmalig von dem Vorgang in Kenntnis gesetzt. In Beantwortung meines daraufhin übergebenen Fragenkatalogs vom 2. April 2009 hat das Justizministerium seine Auffassung zum Missbrauchsrisiko der verlorenen Daten dargestellt. Demnach sei das „Risiko eines Auslesens oder sonstigen Verwertens durch Unbefugte praktisch auszuschließen“, weil „ohne Kenntnis des Aufbaus der Baumstruktur, der Linearisierungsvorschrift und der intern verwendeten Datentypen dieser

Datenstrom praktisch nicht interpretiert werden kann.“ Erst nach meinem Hinweis auf Software-Tools, die das Auslesen der Daten auch ohne Kenntnisse der Original-Verarbeitungsumgebung für Jedermann ermöglichen, hat das Justizministerium meiner Auffassung zugestimmt, dass nur eine dem Stand der Technik entsprechende kryptographische Verschlüsselung einen angemessenen Schutz der Daten während des Transports darstellt, und angesichts des tatsächlich bestehenden Missbrauchsrisikos eine Information der Betroffenen erforderlich ist.

Das Justizministerium hat mit der Fa. R. einen Vertrag nach dem Muster der Besonderen Vertragsbedingungen für die Pflege von DV-Programmen (BVB-Pflege-Vertrag) über die Wartung und Pflege der Anwendung für das Elektronische Grundbuch abgeschlossen. Eine Ausfertigung des Vertrages wurde mir am 13. Juli 2009 zur Verfügung gestellt. Dieser läuft vom 1. Januar bis 31. Dezember 2008 und enthält keine Vereinbarungen über technisch-organisatorische Maßnahmen zur Sicherstellung des Datenschutzes bei Wartungsarbeiten. Lediglich die Standardklausel des BVB-Pflegevertrages verpflichtet den Auftragnehmer zur Beachtung der gesetzlichen Bestimmungen zum Datenschutz (§ 11). Darüber hinaus ist zwar eine Vertragsstrafe vereinbart, die „bei einem Verstoß des Auftragnehmers gegen eine Datenschutzvorschrift oder eine Sicherheitsvereinbarung“ fällig wird, jedoch wird auch dies nicht konkretisiert. Insbesondere ist kein Verweis auf Sicherheitskonzepte oder andere für den technischen und organisatorischen Datenschutz maßgebliche Dokumente enthalten.

Einen aktualisierten Vertrag für das Jahr 2009, wieder mit einer Laufzeit von 12 Monaten, erhielt ich mit Schreiben vom 14. Oktober 2009. Dieser Vertrag enthält nunmehr ergänzenden Regelungen zur Verarbeitung personenbezogener Daten im Auftrag.

Mit Schreiben vom 17. August 2009 hat das Justizministerium das Sicherheitskonzept (§ 22 Abs. 5 DSGVO M-V) für das Elektronische Grundbuch in der Version 1.0 mit Bearbeitungsstand 20. Juni 2006 vorgelegt. Basis für das Sicherheitskonzept ist eine Risikoanalyse mit Stand vom 25. Februar 2004. Das Konzept weist allerdings große Lücken auf. Eine große Zahl von Modulen ist unbearbeitet, insbesondere fehlen die als notwendig erachteten Regelungen für Wartungs- und Reparaturzwecke (z. B. Baustein B 3.01, Maßnahme M 2.4).

Zusammen mit einer Bewertung des Entwurfs dieser Beanstandung erhielt ich am 30. September 2009 vom Justizministerium ein Dokument, das Hinweise zur Fortschreibung des Sicherheitskonzeptes enthält. Werden diese Hinweise vollständig berücksichtigt ist davon auszugehen, dass das Sicherheitskonzept die Anforderungen des § 22 Abs. 5 DSGVO M-V erfüllt. Vordringliche Teilaspekte sind bereits abschließend bearbeitet. So ist der Umgang mit mobilen Datenträgern neu geregelt worden und sowohl im Betriebshandbuch (siehe unten) als auch in einem weiteren Papier („Empfehlungen zum Umgang mit Mobilien Datenträgern“) dokumentiert.

Am 12. September 2008 habe ich die erste Version des Betriebshandbuchs der Fa. D. erhalten, welches die dortigen betriebsinternen Verfahren und Regelungen beschreibt. Auch dieses Dokument enthielt zu diesem Zeitpunkt keine detaillierten Regelungen für Wartung und Störungsbeseitigung und insbesondere keine Vorgaben zur Datensicherheit und zum Datenschutz bei der Nutzung von Grundbuch-Echtdaten für Zwecke der Wartung, Reparatur oder Störungsbeseitigung.

Mit dem o. g. Schreiben vom 30. September 2009 übergab mir das Justizministerium eine aktualisierte Version des Betriebshandbuchs (Version 2.2, Stand September 2009). Der Umgang mit Datenbankexporten und die Vorgaben für die jetzt eingesetzten USB-Sticks sind nunmehr darin dokumentiert.

Eine Freigabeerklärung (§ 19 Abs. 1 DSGVO M-V) und eine Verfahrensbeschreibung (§ 18 Abs. 1 DSGVO M-V) für das Verfahren A. lag zum Zeitpunkt des besagten Vorfalls nicht vor. Das Justizministerium vertritt die Auffassung, dass die Vorschriften des DSGVO M-V auf den Betrieb des elektronischen Grundbuches nicht

anwendbar sind. Dennoch hat es eine inzwischen eine Verfahrensbeschreibung in Anlehnung an § 18 DSG M-V angefertigt und mir ebenfalls mit dem Schreiben vom 30. September 2009 übergeben. Zudem erwägt das Justizministerium, nach der Überarbeitung des Sicherheitskonzeptes eine Freigabeerklärung zu erstellen.

Das Justizministerium hat mich inzwischen darüber informiert, dass die in den o. g. Dokumenten beschriebenen, verbesserten Verfahren zur Erstellung und zur Übergabe der Datenbankexporte in der Fa. D. jetzt angewendet werden. Insbesondere werden die Daten nun kryptographisch verschlüsselt für den Transport bereitgestellt. Ferner werden die einzelnen Arbeitsaufgaben stärker formalisiert und zwischen den Verfahrensbetreuern und dem zentralen Datenein- und -ausgang neu aufgeteilt, so dass eine bessere Nachweisführung gegeben ist.

Nach Abschluss des staatsanwaltschaftlichen Ermittlungsverfahrens wurden die betroffenen Grundstückseigentümer – jedoch nicht persönlich – gem. § 23 DSG M-V in Kenntnis gesetzt. Die Datenbanken enthalten regelmäßig keine aktuellen Adressen der Grundstückseigentümer, soweit diese nicht selbst auf dem Grundstück wohnen, und auch nicht sonstiger Berechtigter. Aufgrund der großen Anzahl von 34.000 betroffenen Grundbüchern wurde in Absprache mit mir der Verlust des USB-Sticks am 10. August 2008 durch Aushang in den Amtsgerichten Demmin und Ribnitz-Damgarten und durch eine entsprechende Mitteilung im Amtlichen Anzeiger Nr. 32 vom 10. August 2009 öffentlich bekannt gemacht sowie durch eine Pressemitteilung begleitet.

## **B) Gründe:**

### **Anwendbarkeit des DSG M-V**

Entgegen der Auffassung des Justizministeriums, zuletzt geäußert im Schreiben vom 30. September 2009, halte ich die Vorschriften des DSG M-V für anwendbar. Gemäß § 2 Abs. 4 Satz 2 gilt dieses Gesetz für die Gerichte, „soweit sie Verwaltungsaufgaben wahrnehmen.“ Das Führen der Grundbücher ordnet die so genannte Hamburger Liste zwar den Rechtspflegeaufgaben zu. Die Umsetzung der technischen und organisatorischen Maßnahmen zur Datensicherung ist jedoch der äußeren Ordnung und damit den Verwaltungstätigkeiten zuzuordnen und unterliegt somit der Kontrollkompetenz des Landesbeauftragten für den Datenschutz.

Selbst wenn man der Auffassung des Justizministeriums folgen würde, dass die derzeitigen Regelungen des DSG M-V auf den Betrieb des Elektronischen Grundbuchs nicht anwendbar wären, würde hier kein rechtsfreier Raum entstehen, da in diesem Fall das Bundesdatenschutzgesetz (BDSG) zur Anwendung käme. Gem. § 1 Abs. 2 Nr. 2 b gilt das BDSG auch für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesrecht geregelt ist und soweit sie als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungstätigkeiten handelt. Damit hätten für das Verfahren Elektronisches Grundbuch technische und organisatorische Maßnahmen gem. § 9 BDSG und Anlage getroffen werden müssen. Die in § 9 normierte Erforderlichkeit und Angemessenheit dieser Maßnahmen ist nur durch systematisches und konzeptionelles Vorgehen bei deren Auswahl belegbar, bspw. im Sinne der Grundschutzmethodik des BSI, so dass auch aus den Regelungen des BDSG die Notwendigkeit der Erstellung eines Sicherheitskonzeptes ableitbar ist.

Von einer Beanstandung wegen Verstößen gegen die Pflichten zur Erstellung einer Verfahrensbeschreibung (§ 18 Abs. 1 DSG M-V), zur Erstellung eines Sicherheitskonzeptes (§ 22 Abs. 5 DSG M-V) und zur Freigabe (§ 19 Abs. 1 DSG M-V) sehe ich gem. § 32 Abs. 2 DSG M-V jedoch ab, da die Mängel inzwischen weitgehend beseitigt sind. Die erforderlichen Unterlagen sind z. T. bereits erstellt bzw. in Bearbeitung. Zudem gehe ich

davon aus, dass eine formelle Freigabe des Verfahrens erfolgen wird, sobald alle hierfür erforderlichen Unterlagen vorliegen.

#### Zu 1.

Das Justizministerium hat bei der Ausgestaltung und -durchführung des Verfahrens der Führung des Elektronischen Grundbuches wesentliche Vorgaben zur Datenverarbeitung im Auftrag aus § 4 DSG M-V verletzt.

##### *a) Vertragsgrundlagen*

Das Justizministerium hat den Auftrag an die Fa. R. nicht im erforderlichen Umfang schriftlich erteilt, Art und Umfang der Verarbeitung personenbezogener Daten waren jedenfalls nicht hinreichend bestimmt festgelegt und es fehlten gesetzlich erforderliche ergänzende Weisungen zu technischen und organisatorischen Maßnahmen (§ 4 Abs. 1 Satz 4 DSG M-V). Vorgaben zum Schutz personenbezogener Daten im Rahmen von Wartung und - soweit zutreffend - Fernwartung (vgl. § 4 Abs. 4 DSG M-V) fehlten vollständig.

##### *b) Eignung der Fa. R. als Auftragnehmer*

Laut Aussage des Staatssekretärs des Justizministeriums hat die Fa. R. den Transport der Datenbankexporte als hinreichend gesichert veranlasst und noch nach dem Vorfall eine Auslesemöglichkeit der Daten durch Unbefugte ausgeschlossen. Damit ist ihre Eignung als Auftragnehmer im Sinne von § 4 Abs. 1 Satz 3 DSG M-V neu zu bewerten.

##### *c) Eignung der Fa. D. als Auftragnehmer*

Die Fa. D. hat einen unverschlüsselten Transport der Datenbankexporte unwidersprochen hingenommen und den Verlust des USB-Sticks durch einen ihrer Mitarbeiter zu verantworten. Als Ursache für das Abhandenkommen steht zweifelsfrei ein Verstoß des verantwortlichen Mitarbeiters der Fa. D. gegen die betriebsinternen Regelungen zur Aufbewahrung von mobilen Datenträgern außerhalb der Dienstzeit fest. Der Umgang der Fa. D. mit diesem Vorfall ist jedoch in keiner Weise zu beanstanden. Insbesondere wurden inzwischen alle erforderlichen Maßnahmen getroffen, um eine Wiederholung möglichst auszuschließen. Vor diesem Hintergrund wird die Eignung der Fa. D. als Auftragnehmer nicht in Frage gestellt.

#### Zu 2.

Mit der Duldung des Transports von unverschlüsselten Datenbankexport-Dateien zwischen den Auftragnehmern hat das Justizministerium gegen seine Pflicht zur Ergreifung von dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen zur Sicherung der Vertraulichkeit aus § 21 Abs. 2 Nr. 1 DSG M-V verstoßen.

Die personenbezogenen Daten der Grundbücher sind so zu schützen, dass sie nur bei berechtigtem Interesse zugänglich sind (§ 12 Grundbuchordnung). Daher sind Maßnahmen zur Sicherung der Vertraulichkeit zu treffen.

Das gewählte Datenformat (Exportformat der Datenbank) ist zur Sicherung der Vertraulichkeit ungeeignet. Dieses Datenformat verhindert nicht, dass Jedermann mit Datenbankkenntnissen, auch ohne konkrete Kenntnisse der verwendeten Anwendung, die Inhalte lesbar machen kann. Auch die Kompression von Daten ist keine geeignete Maßnahme zur Sicherung der Vertraulichkeit.

Weiterhin ist jedoch der Umstand, dass die Daten unverschlüsselt transportiert werden sollten, ein besonderes Risiko. Jedermann ist mit frei verfügbarer Software und bestimmten Fachkenntnissen in der Lage,

die Datenbankinhalte wie Namen, Vornamen und Geburtsdaten der Grundstückseigentümer, ehemaliger Eigentümer sowie eingetragene Belastungen durch Kredite und Rechte am Grundstück auszulesen. Diese können damit konkreten Personen zugeordnet werden.

#### **Zur Frage der Benachrichtigung Betroffener**

Der Zeitpunkt und die Form der Benachrichtigung der Betroffenen ist nicht zu beanstanden.

Gemäß § 23 DSGVO hat eine Daten verarbeitende Stelle die Betroffenen **unverzüglich** zu benachrichtigen, wenn sie Grund zu der Annahme oder Kenntnis hat, „dass unrichtige, unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten in der Weise genutzt wurden, dass dem Betroffenen daraus ein Nachteil entstanden ist oder zu entstehen droht.“ Das Justizministerium hat spätestens am 12. März 2009 vom Verlust des Datenspeichers Kenntnis erlangt. Aufgrund der darauf enthaltenden personenbezogenen Angaben zu Grundstückseigentümern und deren rechtlichen und finanziellen Verhältnissen droht den Betroffenen ein Nachteil zu entstehen. Daten, die gemäß § 12 GBO nur bei Vorliegen und Glaubhaftmachung eines berechtigten Interesses durch die Grundbuchämter herausgegeben werden können, standen nunmehr möglicherweise auch unberechtigten Dritten zur Verfügung.

Darüber sind Betroffene unverzüglich, also ohne schuldhaftes Zögern, zu informieren. Die Information der Betroffenen kann zu einer Erhöhung der Gefahr führen, wenn der ggf. unberechtigte Besitzer des abhanden gekommenen USB-Sticks erst durch die öffentliche Benachrichtigung von der Brisanz des erlangten Datenspeichers erfährt und erst hierdurch Anstrengungen unternimmt, sich die Daten zugänglich zu machen.

Mit der Einstellung der staatsanwaltschaftlichen Ermittlungen am 27. Juli 2009 wegen fehlender Ermittlungsansätze konnte davon ausgegangen werden, dass der Erfolg strafrechtlicher Maßnahmen nicht mehr gefährdet würde. Die Information der Betroffenen erfolgte am 10. August 2008 durch Aushang in den Amtsgerichten Demmin und Ribnitz-Damgarten und durch eine entsprechende Mitteilung im Amtlichen Anzeiger Nr. 32 vom 10. August 2009 und wurde durch eine Pressemitteilung begleitet.

#### **C) Mit dieser Beanstandung verbinde ich folgende Empfehlungen:**

1. Die Verfahrensweisen Fa. R. bei der Pflege und Wartung der Software A. sollten überprüft werden. Hierbei ist besonders zu untersuchen, ob die von § 4 Abs. 1 Satz 3 DSGVO geforderte Eignung für die Gewährleistung technischer und organisatorischer Datenschutzmaßnahmen vorliegt. Geeignete Instrumente zu dieser Prüfung sind insbesondere einschlägige Datenschutz- und IT-Sicherheitskonzepte des Unternehmens.
2. Es ist ein Vertrag zu schließen, der die in § 4 DSGVO genannten Forderungen umsetzt. Ich empfehle, sich beim Vertragstext an dem Muster auf meiner Website zu orientieren ([http://www.datenschutz-mv.de/dschutz/musterve/mv\\_dviau.html](http://www.datenschutz-mv.de/dschutz/musterve/mv_dviau.html)).
3. Es ist ein geeignetes Produkt zur Verschlüsselung der im Rahmen der Wartung und Pflege zu übertragenden personenbezogenen Daten auszuwählen. Die Handhabung des Produktes ist schriftlich festzulegen.
4. Um den Umfang der zu übertragenden Daten zu reduzieren sollten auch andere technische Möglichkeiten geprüft werden, beispielsweise die Fernwartung durch einen Dienstleister, jeweils auf Anforderung und

unter der Kontrolle der Fa. D. Mitarbeiter der Fa. R. könnten auch in den Räumen der Fa. D. arbeiten, wenn geeignete Zugangs- und Zutrittsschutzmaßnahmen ergriffen werden.

5. Das Sicherheitskonzept (§ 22 Abs. 5 DSG M-V) ist zu aktualisieren, insbesondere sind die noch nicht bearbeiteten Module einschließlich Zugriffsschutzkonzept einzuarbeiten. Die Verfahrensbeschreibung (§ 18 Abs. 1 DSG M-V) für das Verfahren A. ist zu erstellen und das Verfahren ist formell gemäß § 19 Abs. 1 DSG M-V freizugeben.
6. Das Zugriffsrechtekonzept ist zu erstellen bzw. überarbeiten, sofern die entsprechenden Details nicht dem Sicherheitskonzept zu entnehmen sind.