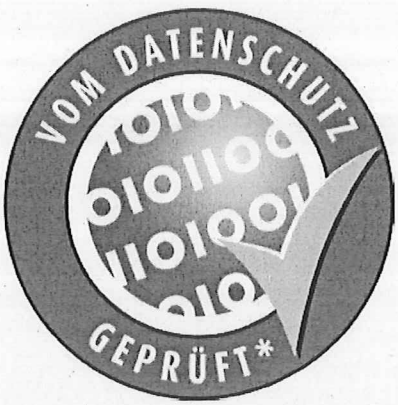

Öffentliches Gutachten

Reauditierung im Auditverfahren gemäß § 43 Abs. 2 LDSG

Zutrittsberechtigungssystem und Videoanlage für das Landeshaus Kiel und Karolinenweg 1

Erstellungsdatum: 14. Juli 2014

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Autor:	Henry Krasemann / Dr. Thomas Probst
Tel.:	0431-988 1200
Fax:	0431-988 1223
E-Mail:	audit@datenschutzzentrum.de
Datum:	14.07.2014
Version:	1.0

Inhaltsverzeichnis

1 Datenschutz-Behördenaudit: Reauditierung 2014

Nach der Erstauditierung des Zutrittsberechtigungssystems des Landtages am 23.09.2004 wurde die Auditierung am 28.08.2006 auf die Videoanlage des Landtages Schleswig-Holstein ausgedehnt; gleichzeitig wurde das Zutrittsberechtigungssystem reauditiert. Eine weitere Reauditierung erfolgte am 15.03.2010.

Die vorliegende Reauditierung umfasst weiterhin beide Bestandteile. Im Detail werden das Zutrittsberechtigungssystem des Landeshauses, Düsternbrooker Weg 70, und des Gebäudes Karolinenweg 1 in Kiel sowie die Videoüberwachung dieser Gebäude, der zum Landeshaus gehörenden Tiefgarage und des Parkhauses Reventlouallee in Kiel reauditiert.

1.1 Änderung am Auditgegenstand: IDS

Änderungen am Auditgegenstand betrafen insbesondere die Abschaltung des Intrusion Detection Systems (IDS). Dieses war am Netz „secLAN" angeschlossen, das als eigenständiges Netz die Komponenten des Zutrittsberechtigungssystems und der Videoüberwachung miteinander verbindet. Das IDS diente der Erkennung von Einbruchs- und Angriffsversuchen durch Beobachtung des Datenverkehrs. Grund für die Abschaltung war, dass diese Erkennung nach Aussage der Landtagsverwaltung nur unzureichend funktionierte und eine kostenintensive Wartung sowie die umfangreichen Updatemaßnahmen nicht rechtfertigen würde. Als Alternative soll das Netz „secLAN" auf unbefugte Netzteilnehmer überwacht werden. Außerdem werden die Switche nach Aussage der Landtagsverwaltung regelmäßig administriert und gehärtet, so dass Konfigurationsänderungen durch unbefugte Netzteilnehmer unterbunden werden. [...]

Nur Administratoren sowie die Nutzer der Videoüberwachung und die (Fach-)Administration des Zutrittsberechtigungssystems kämen mit der Infrastruktur des secLAN in Berührung. Dies rechtfertige den Verzicht auf das IDS.

1.2 Vor-Ort-Besichtigung

Im Rahmen einer Vor-Ort-Besichtigung am 15.08.2013 haben wir festgestellt, dass das Ausblenden der Videobereiche außerhalb des Geländes des Landtags dejustiert war und dadurch weite Teile der Kiellinie und des Düsternbrooker Wegs einsehbar wurden. [...] Grund für die Dejustierung waren vermutlich Vibrationen und die zahlreichen Kamerabewegungen im laufenden Betrieb, wodurch sich der Nullpunkt verschoben hatte. Aufgrund dieser Feststellung wurde ein weiterer Vor-Ort-Termin (21.11.2013) vereinbart, bei dem auch ein Techniker der Firma anwesend war, die für die Einrichtung der Videoanlage verantwortlich ist. Hierbei erfolgte eine erste grobe Neujustierung. Zwar ist ein vollständiges Ausblenden der nicht für die Überwachung vorgesehenen Bereiche nicht möglich. [...] Eine Verfolgung der Personen ist wesentlich erschwert. Inzwischen wurden uns auch Screenshots hiervon übermittelt, die dieses dokumentieren. Hierbei ist zu beachten, dass es sich sowohl bei der Kiellinie als auch beim Düsternbrooker Weg um Wege handelt, auf denen nur gelegentlich Personen länger verweilen und keine Bereiche erhöhter Sensibilität erfasst werden. Die nunmehr erfolgte Ausblendung reicht daher u. E. für einen datenschutzkonformen Einsatz aus.

Um weitere derartige Vorfälle der Dejustierung zu vermeiden, wird nunmehr regelmäßig [...] die Fachfirma die Einstellung überprüfen. Außerdem wurden die Mitarbeiterinnen und Mitarbeiter, die mit der Videoüberwachung beschäftigt sind, in Form einer schriftlichen Arbeitsanweisung aufgefordert, Dejustierungen umgehend zu melden.

1.3 Auswechselung der eingesetzten Chip-Karten

Schon bei der letzten Reauditierung wurde vom ULD darauf hingewiesen, dass die eingesetzten MIFARE-Classic-Karten als nicht mehr sicher anzusehen sind, weil die dort eingesetzte Verschlüsselung gebrochen wurde. Nunmehr wurden die sicherheitsrelevanten Zugänge Mitte 2011 auf das MIFARE-DESFire-Leseverfahren (EV1-Chip) umgestellt. [...]

Das MIFARE-DESFire-Leseverfahren arbeitet mit einer 128-Bit-AES-Verschlüsselung. Unverschlüsselt hingegen ist weiterhin die jeweils einmalige UID-Nummer der Karte. Diese wird im Bereich der Obersten Landesbehörden für die elektronische Zeiterfassung genutzt und gehört nicht zum Auditierungsgegenstand. Im Landeshaus wird die UID nicht verwendet.

Für das Zutrittsberechtigungssystem wird stattdessen die auf der Karte aufgedruckte Nummer (nicht die UID) verwendet, die verschlüsselt auf der Karte gespeichert ist. Sie kann kontaktlos nur ausgelesen werden, wenn im Lesegerät der entsprechende Schlüssel vorhanden ist. Auf dem Kartenchip selbst befinden sich ansonsten nur Nutzdaten aus dem Kantinenbereich (u. a. die eingezahlte Geldmenge).

Ein Auslesen der Karte ist nach Aussage der Landtagsverwaltung nur durch nahezu direkten Kontakt der Karten mit dem Lesegerät möglich.

Für das Abrechnungssystem in der Kantine wird eine ebenfalls die MIFARE-Classic-Emulation auf der Karte verwendet. Damit ist es möglich, dass die neuen Karten auch noch mit den alten Lesegeräten genutzt werden können. Das Abrechnungssystem in der Kantine gehört nicht zum Auditgegenstand. [...]

Die Umstellung auf die neuen Chips bzw. das neue Kartensystem ist begrüßenswert. Das Auslesen der Karten, und damit die Ermöglichung einer unzulässigen Zutrittsberechtigung, wird deutlich erschwert. Dass die nicht verschlüsselte UID teilweise für die Zeiterfassung genutzt wird, halten wir für akzeptabel aufgrund des geringen Missbrauchsrisikos bzw. des geringen drohenden Schadens durch Missbrauch. Inzwischen wurde der folgende Abschnitt in die Ausgabehinweise aufgenommen, die jeder Besitzer einer Karte erhält:

„Verbleibendes Risiko

Auf die Karte kann nur in unmittelbarer Nähe zu einem Lesegerät zugegriffen werden. Das Risiko, dass die Karte darüber hinaus erkannt wird, lässt sich nicht vollständig ausschließen. Das ULD empfiehlt daher – wie bei allen kontaktlosen Karten – die Verwendung einer speziellen Schutzhülle, die keine Kommunikation zwischen Karte und Außenwelt zulässt.

Derartige Schutzhüllen können über den Fachhandel bezogen werden."

1.4 Ablauf der Gültigkeit der Karten

Im Rahmen des Reauditierungsverfahrens haben wir gegenüber der Landtagsverwaltung die Dauer der Aufbewahrung von Stammdaten hinterfragt. Diese werden bei Rückgabe der Karte gelöscht. Erfolgt jedoch keine Rückgabe, so erfolgte die Löschung erst nach [...] nach Ablauf der Gültigkeit der Karte. Diese Frist wurde nun auf [...] verkürzt. Hierzu führt die Landtagsverwaltung [...] an: „Betroffen ist grundsätzlich eine Personengruppe. Es geht um die [...]. Die ausgegebenen Karten an die [...] sind [...] befristet/gültig. Bei jeder ‚Verlängerung' tauchen [...] bzw. Inhaber dieser Karten auf, die plötzlich feststellen, dass ihre Karte nicht mehr berechtigt ist. In diesen Fällen wird dann die Verlängerung vollzogen. Im Übrigen kann lediglich über das System festgestellt werden, bis wann die Karte funktionsfähig = gültig war. Wäre diese Frist kürzer, z. B. [...], müsste der Administrator die erforderlichen Daten wieder komplett neu eingeben. Die Dauer von [...] stellt somit für uns eine Vereinfachung dar, sie reduziert den Verwaltungsaufwand."

Außerdem wurden die Ausgabehinweise dahingehend geändert, dass die Rückgabe der Karte nicht nur beim Ausscheiden einer Mitarbeiterin oder eines Mitarbeiters erfolgen muss, sondern auch „bei Wegfall der Erforderlichkeit (z. B. [...])".

Mit Blick darauf, dass der Karteninhaber die Löschung seiner Stammdaten mit Rückgabe der Karte selbst in der Hand hat, halten wir diese Frist für akzeptabel.

1.5 Sonstige Änderungen

Des Weiteren wurde die Hardwareausstattung in der Pförtnerloge und an sonstigen Arbeitsplätzen aktualisiert. Hieraus ergibt sich keine Änderung an der Datenverarbeitung.

Außerdem wurde die Videotechnik mit [...] Infrarot-Strahlern ergänzt. Diese betreffen [...] Kamerastandorte [...] des Landeshauses. Die Strahler erzeugen „unsichtbares" Licht und führen zu einer Verbesserung der Videoqualität bei Dunkelheit. Eine Ausweitung der Videoüberwachung ist hiermit nicht verbunden, so dass sich hieraus auch keine Änderung der rechtlichen Bewertung ergibt.

1.6 Änderung der gesetzlichen Lage

Zum 01.01.2009 trat die Datenschutzverordnung 2009 (DSVO 2009) in Kraft, die für automatisierte Verfahren Details und Umfang der Verfahrensdokumentation und der Dokumentation von Sicherheitsmaßnahmen sowie von Test und Freigabe regelt. Sofern keine wesentlichen Änderungen eines Verfahrens erfolgen, hatte eine Anpassung der Dokumentation bis zum 31.12.2011 zu erfolgen.

Die Dokumentation wurde stichprobenartig anhand der Vorgaben der DSVO 2009 überprüft. Dabei wurden keine Mängel festgestellt.

Das LDSG wurde am 15.09.2011, 11.01.2012 und 06.04.2013 geändert. Die Änderungen betrafen u. a. die allgemeinen Maßnahmen zur Datensicherheit (§ 5 LDSG) und neue Vorgaben für die Video-Überwachung und Aufzeichnung (§ 20 LDSG). Die Auswirkungen auf den Auditgegenstand werden in Kapitel 3 dargestellt und bewertet.

Außerdem trat die Datenschutzordnung des Schleswig-Holsteinischen Landtages (DSO SH) am 27.04.2013 in Kraft. Nach § 1 Abs. 2 S. 1 und S. 2 Nr. 2 und 3 DSO SH gilt allerdings das Landesda-

tenschutzgesetz für die Bereiche Personalverwaltung des Landtags und Ausübung des Hausrechts und der Ordnungsgewalt gemäß Artikel 14 Abs. 3 Satz 2 der Landesverfassung. Somit findet auf das Zutrittsberechtigungssystem und Videoanlage für das Landeshaus Kiel das LDSG Anwendung.

2 Fortentwicklung des Datenschutzmanagementsystems

2.1 Datenschutzziele

Im Rahmen des Datenschutzmanagementsystems wurden bei den (Re-)Auditierungen 2006 und 2010 sechs aktuelle Datenschutzziele formuliert, die neben allgemeinen Daueraufgaben des Datenschutzmanagements umzusetzen waren. Im Einzelnen sind dies:

1. Die Gewährleistung einer funktionierenden Videoanlage /-überwachung innerhalb des Zutrittsberechtigungssystems unter Einhaltung der erstmals in dem Konzept vom 15.09.2005 Version 249 festgelegten Bedingungen

2. Analoge Ergänzung/Fortschreibung der Dienstanweisungen für das ZBS vom 19.04.2006 um die Systeme der Videoanlagen bezüglich der Verwaltung, Administration und den Kontrollmaßnahmen

3. Dienstanweisung für den Zugriff auf das Archiv der gespeicherte Aufnahmen gem. Konzept

4. Dienstanweisung/Verfahrensregelung für die Herausgabe von gespeicherten Videoaufnahmen und deren rechtliche Prüfung

5. Erstellung einer Information an die Mitarbeiter in der Pförtnerei bezüglich der durch Dienstanweisung geregelten Aufsicht/Kontrolle über das Schwenk- und Zoom-Verhalten

6. Test und Freigabe der Videoanlage innerhalb des ZBS.

Dies war schon bei der letzten Reauditierung in Form einer Dienstanweisung geschehen, die genaue Vorgaben für die Administration und Nutzung des Zutrittberechtigungssystems und für die Nutzung, Auswertung und Weitergabe von Aufzeichnungen der Videoanlage macht. Weiterhin wurde das Gesamtsystem durch den Landtagspräsidenten freigegeben. Damit wurden die notwendigen Anpassungen der o. g. Dokumente umgesetzt.

2.2 Regelmäßige Kontrollen

Die Mitarbeiterinnen und Mitarbeiter der Pförtnerei können die installierten Dome-Kameras schwenken sowie den Bildausschnitt verändern (Zoom). Dies ist ihnen erlaubt, um mögliche Gefährdungen zu erkennen; das bewusste Verfolgen und Beobachten von Personen ohne Gefährdungspotential ist hingegen untersagt. Durch Mitarbeiterinnen und Mitarbeiter der Landtagsverwaltung erfolgt eine stichprobenartige Kontrolle des Schwenk- und Zoom-Verhaltens der Mitarbeiterinnen und Mitarbeiter der Pförtnerei. Hierzu kann sich die bzw. der zuständige Mitarbeiterin /

Mitarbeiter der Landtagsverwaltung [...] auf das aktuelle Kamerabild aufschalten.

Dem Datenschutzgremium wurden im Berichtszeitraum die entsprechenden Protokolle ausreichend häufig vorgelegt. Hierüber wurden entsprechende Vermerke erstellt.

Hinsichtlich der Verwendung der aufgezeichneten Daten für die Verfolgung von Straftaten [...] wurde uns mitgeteilt, dass die Videobilder maximal [...] aufbewahrt werden. Pro Jahr käme es zu ca. [...] Anfragen. Die Einsichtnahme erfolgt nach dem Vier-Augen-Prinzip. Die erste Person soll aus dem Bereich [...] stammen, die zweite Person aus dem Bereich [...] sein. Zur Abwehr einer Gefahr darf vom Vier-Augen-Prinzip abgewichen werden. Der Zugriff erfolgt mit Hilfe eines [...] hinterlegten Passwortes, dessen Benutzung ([...]) protokolliert wird. Die Vergabe eines neuen Passwortes nach Benutzung durch die Systemadministration [...] ist organisatorisch geregelt. Eine entsprechende Dienstanweisung wurde im Rahmen des Datenschutzmanagements erstellt Die Protokolle über die Einsichtnahmen nach dem Vier-Augen-Prinzip wurden uns vorgelegt.

2.3 Dokumentation

Im Rahmen der Reauditierung wurden die Dokumentation sowie Aufzeichnungen und Protokolle geprüft. Die relevante Dokumentation besteht aus einem fortgeschriebenen Feinkonzept für das Zutrittsberechtigungssystem und die Videoanlage sowie aus Dienstanweisungen für die technische Administration der Systeme, die fachliche Administration und die Pförtnerei.

Die Anpassung der Dokumentation wurde im Rahmen der letzten Reauditierung als Datenschutzziel formuliert und ist inzwischen erfolgt (siehe u. a. Schreiben der Landtagsverwaltung vom 10.02.2010). Dies betraf folgende Dokumentationen:

- Dokumentation der zur Inbetriebnahme der verwendeten Programme getätigten Schritte (§ 3 Abs. 2 Nr. 3 2. HS DSVO),
- Dokumentation der Änderungen einschließlich der Personen, die die Änderungen vorgenommen haben (§ 3 Abs. 2 Nr. 6 DSVO),
- Fortschreibung der Dokumentation bei Änderungen und Aufbewahrung mindestens fünf Jahre nach der letzten automatisierten Verarbeitung personenbezogener Daten (§ 3 Abs. 3 DSVO).

Diese Dokumente wurden eingesehen und stichprobenartig geprüft. Dabei wurden keine Mängel festgestellt.

3 Datenschutzrechtliche Bewertung

Das ULD hat im Rahmen der Prüfung festgestellt, dass die technischen und organisatorischen Sicherheitsmaßnahmen des Zutrittsberechtigungssystems und der Videoanlage für das Landeshaus Kiel ein unverändert hohes Niveau haben.

Innerhalb des Berichtszeitraums März 2010 bis November 2013 wurden am Auditgegenstand nur kleinere Änderungen durchgeführt. Wesentliche Änderungen im Sinne der „Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG", die eine frühzeitige Reauditierung durch das ULD erfordert hätten, wurden sowohl gemäß Konzeptlage als auch bei den stichprobenartigen Kontrollen nicht festgestellt.

Im Rahmen der Regelungen zu den allgemeinen Maßnahmen zur Datensicherheit wurde das LDSG während des Gültigkeitszeitraums u. a. hinsichtlich der Ausformulierung von Schutzzielen geändert. Diese Vorgaben nach § 5 Abs. 1 S. 2 LDSG muss auch der Auditgegenstand einhalten:

Im Rahmen der **Verfügbarkeit** müssen Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können. Hinsichtlich des Zutrittsberechtigungssystems werden die Risiken bzgl. des Ausfalls des Systems im Feinkonzept beschrieben und bewertet. Bei Stromausfall ist das Verlassen des Gebäudes über die Fluchtwege weiterhin gewährleistet. Bzgl. der Videoüberwachung spielt die Verfügbarkeit nur eine untergeordnete Rolle, da es sich hierbei nur um eine unterstützende Maßnahme im Rahmen des Gesamtsicherheitskonzepts handelt, die übergangsweise auch etwa durch menschliche Beobachtung ersetzt werden kann.

Im Rahmen der **Integrität** müssen die Daten unversehrt, vollständig, zurechenbar und aktuell bleiben. Hinsichtlich des Zutrittsberechtigungssystems sind die Mitarbeiterinnen und Mitarbeiter des Landeshauses und auch die sonstigen Empfänger der Karten (z. B. Pressevertreter) gehalten, einen Verlust von Karten umgehend zu melden. Auch im Fall des Ausscheidens müssen die Mitarbeiterinnen und Mitarbeiter bzw. bei Wegfall der Erforderlichkeit bei Pressevertretern ihre Karten zurückgeben (siehe Dokument „Ausgabehinweise"). Es wurden sowohl bzgl. des Zutrittsberechtigungssystems als auch der Videoüberwachung technische Vorkehrungen zur Verhinderung von Manipulation getroffen (siehe Feinkonzept).

Im Rahmen der **Vertraulichkeit** darf nur befugt auf Verfahren und Daten zugegriffen werden. Hinsichtlich des Zutrittsberechtigungssystems wird nur in einem sehr eingeschränkten Maße protokolliert ([...]), so dass die gespeicherten Daten auf das minimal Erforderliche reduziert sind. Bei der Videoüberwachung erfolgt eine automatische Löschung der Aufzeichnungen nach [...]. Es besteht ein Rechtemanagement bzgl. des Zugriffs auf die Daten (siehe Feinkonzept).

Im Rahmen der **Transparenz** muss die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen werden können. Zugriffe auf Daten werden protokolliert und die Protokolle einem Datenschutzgremium mindestens einmal jährlich zur Kontrolle vorgelegt. Das Feinkonzept, Dienstanweisungen und Hinweisblätter dokumentieren die Verfahren und stellen auch gegenüber Betroffenen Transparenz her.

Im Rahmen der **Nicht-Verkettbarkeit** dürfen personenbezogene Daten nicht oder nur mit unver-

hältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden. Einer Verkettbarkeit wird beim Zutrittsberechtigungssystem schon dadurch entgegengewirkt, dass [...] erfolgt. Im Rahmen der Zweckbindung kann eine Einsichtnahme in die Protokolle oder auch die Videodaten nur entsprechend der Dienstanweisung erfolgen. Auch diese Zugriffe werden protokolliert und geprüft.

Im Rahmen der **Intervenierbarkeit** sind Verfahren so zu gestalten, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 LDSG wirksam ermöglichen. Auskunft über die eigenen Daten kann über ein manuelles Verfahren bei der Landtagsverwaltung gefordert werden. Stammdaten der Chipkarten-Inhaber werden nach Rückgabe der Karte bzw. ansonsten spätestens nach [...] gelöscht. Videoaufzeichnungen werden nach [...] automatisch gelöscht.

Das in der Erstauditierung festgestellte Sicherheits- und Datenschutzniveau wurde und wird zukünftig durch Detailverbesserungen weiter angehoben. Dazu gehört die Anpassung der Dokumentation an den Anforderungen der Datenschutzverordnung (DSVO) 2009.

Die Prüfung hat ergeben, dass Konzepte und Anwendung des Datenschutzmanagementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen geben.

Allerdings ist es erforderlich, dass das Feinkonzept aktualisiert und an die aktuelle Rechtslage angepasst wird. Das aktuelle Dokument entspricht zwar inhaltlich den auch aktuell gelten Rechtsnormen, jedoch werden teilweise noch Gesetze zitiert, die inzwischen geändert wurde. Dies betrifft insbesondere § 20 LDSG. Die neue Regelung zur Videoüberwachung wird weiterhin voll beachtet:

- Die Videoüberwachung ist zur Wahrnehmung des Hausrechts erforderlich (vgl. § 20 Abs. 1 LDSG).
- Der Umstand der Beobachtung und die dafür verantwortliche Stelle sind durch geeignete Maßnahmen (hier durch Schilder) erkennbar gemacht (vgl. § 20 Abs. 2 LDSG).
- Eine kurzfristige Speicherung der Daten für [...] ist erforderlich, um auch nach Feiertagen noch sicherheitsrelevante Vorgänge erkennen zu können. Überwiegende schutzwürdige Interessen der Betroffenen sind in Anbetracht dessen, dass die Auswertung der Daten nach festen Vorgaben protokolliert und überwacht erfolgt, nicht erkennbar (vgl. § 20 Abs. 3 S. 1 LDSG). Eine Nutzung der Bilder erfolgt ansonsten nur zur Verfolgung von Straftaten (vgl. § 20 Abs. 3 S. 2 LDSG).
- Die Löschung erfolgt umgehend nach [...], wenn keine Auffälligkeiten bekannt geworden sind (vgl. § 20 Abs. 5 LDSG).

Die Anpassung der Dokumentation muss bis zur nächsten Reauditierung erfolgen.

Außerdem wurde von der Landtagsverwaltung angekündigt, dass im Zertifizierungszeitraum das im secLAN isolierte (und nicht mit dem Internet verbundene) [...], auf dem die Serverkomponenten des Zutrittsberechtigungssystems ablaufen, durch ein neueres System ersetzt wird. Dies sehen

wir ebenfalls als notwendig an.

Am 01.01.2014 ist eine neue DSVO in Kraft getreten. Nach § 6 DSVO 2014 gilt für bestehende Verfahren eine Übergangsfrist von drei Jahren. Daher muss bis zur nächsten Reauditierung eine Anpassung der Dokumentation an die neuen Vorgaben erfolgen.