# Kurzgutachten

Einhaltung datenschutzrechtlicher Anforderungen
durch das IT-Produkt

## vimacc 2.2 – Video Management Software

der

Accellence Technologies GmbH
Garbsener Landstr. 10
30419 Hannover

erstellt von:


**Andreas Bethke**
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 36 63 000
fax 04822 – 36 63 333
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

**Stephan Hansen-Oest**
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (rechtlich)

Im Tal 10a
24939 Flensburg
tel 0461 – 900 138 21
fax 0461 – 900 138 22
mob 0171 – 2044981
email sh@hansen-oest.com


Stand: Februar 2017

**Inhaltsverzeichnis**

A. Einleitung und Kurzbezeichnung ..... 3
B. Zeitpunkt der Prüfung ..... 3
C. Detaillierte Bezeichnung des Begutachtungsgegenstandes ..... 3
Ausschlüsse und Restriktionen in Bezug auf den Begutachtungsgegenstand ..... 6
D. Tools, die zur Herstellung des IT-Produktes verwendet wurden ..... 7
D. Zweck und Einsatzbereich des Begutachtungsgegenstandes ..... 7
E. Datenflusses ..... 9
E. Zusammenfassung der Prüfergebnisse ..... 10
H. Beschreibung, wie das Produkt den Datenschutz fördert ..... 14

# A. Einleitung und Kurzbezeichnung

In diesem Kurzgutachten werden die Ergebnisse des Zertifizierungsprozesses für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) bezüglich des Videomanagement-Systems **vimacc** der Firma Accellence Technologies GmbH zusammengefasst. Die Prüfung erfolgte mit dem Software-Release 2.2.

Für die Begutachtung wird der Anforderungskatalog in der Version 2.0 zugrunde gelegt.

# B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand in der Zeit vom 08.02.2016 bis 08.02.2017 statt.

# C. Detaillierte Bezeichnung des Begutachtungsgegenstandes

**vimacc** ist eine universelle Videomanagementsoftware zur Übertragung, Anzeige, Auswertung und Archivierung von Videobildern und zugehörigen Metadaten sowie zur Steuerung der Videotechnik wie z.B. Kameras, Encoder und Schaltkontakten eines digital vernetzten CCTV-Systems.

Sie ist eine plattformunabhängige Software für professionelles Videomanagement und kann für komplexe Überwachungslösungen aller Größenordnungen in bestehende IT-Landschaften eingebettet werden.
**vimacc** kann sowohl auf dedizierter Hardware als auch auf virtualisierten Systemen in Rechenzentren eingesetzt werden. Die Software unterstützt folgende Videostandards:
H.263, H.264, H.265, MPEG-4, MJPEG, MxPEG.

Das Produkt bietet neben einer umfangreichen Benutzer- und Rechteverwaltung die Möglichkeit, Video-Streams im Gesamtsystem vollständig und durchgängig zu verschlüsseln. Dabei werden die Video-Streams direkt auf der Kamera (geeignete Kameras vorausgesetzt) mit einem öffentlichen Schlüssel verschlüsselt und erst vom Bediener/Operator entschlüsselt. Hierbei kommt ein Hardware-Dongle (USB) zum Einsatz, auf dem sich ein privater Schlüssel befindet. Die gesamte Übertragung sowie die Speicherung der Streams erfolgt dabei ausschließlich in verschlüsselter Form. Der private Schlüssel selbst ist dabei durch eine PIN geschützt, die BSI-konformen Kennwortrichtlinien unterliegt und sich auf Betreiberseite nicht deaktivieren lässt.

Bei der Verschlüsselung selbst kommt ein hybrides Verfahren aus einer Kombination von RSA und AES zum Einsatz.
Für den Benutzer ist die Verschlüsselung vollständig transparent. Sie führt zu kaum spürbaren minimalen Verzögerungen bei der Übertragung, sodass eine Steuerung von PTZ-Kameras ohne Einschränkungen möglich ist. Die Software beinhaltet in der Auslieferversion keine weiteren Videoanalysemodule, die automatisch personenbezogene Daten erzeugen, verarbeiten oder verknüpfen können.

Um die Verfügbarkeit zu gewährleisten, bietet **vimacc** eine permanente Überwachung der Verbindungen zu den Kameras und signalisiert den Ausfall einer Verbindung umgehend an den Mitarbeiter des Beobachtungs-Arbeitsplatzes und an den technischen Support.

Die grundsätzlichen Funktionen der Software können wie folgt zusammengefasst werden:

- Betrachten von Live-Videoverbindungen und Steuerung von Videokameras
- Wiedergabe von aufgezeichneten Videodaten
- Export von Videodaten
- Konfiguration von Sequenzen und Szenarien
- Setzen von Textmarken
- Arbeiten mit Alarmfällen
- Arbeiten mit Lageplänen

Das Produkt ist in der Lage, Ereignisse bzw. Alarme von verschiedenen Ereignisquellen zu erkennen und selbständig mit konfigurierten Aktionen zu reagieren.
Derartige Ereignisse können beispielsweise sein:

- Ein Notruf wurde ausgelöst.
- Ein Schaltkontakt wurde betätigt.
- Ein Schaltkontakt an einer Kamera wurde betätigt.
- Ein unbefugter Eingriff an der Bildquelle (Kamera verdreht, Gehäuse geöffnet, Rüttelkontakt, usw.) wurde erkannt.
- Eine Bewegung vor einer Kamera (Videosensorik) wurde erkannt.
- Eine technische Störung an der Bildquelle (z.B. Kamerasignal ausgefallen, Festplatten-Füllstand erreicht, usw.) wurde erkannt.
- Ein Routineruf zur Überwachung der Funktionsfähigkeit der Ereignisübertragung von der Bildquelle zur Leitstelle wurde ausgelöst.

Im Zuge einer Alarm- oder Eventverarbeitung können jedem Ereignis bestimmte Aktionen zugeordnet werden. Derartige Aktionen können z. B. Aufschaltungen von Videokameras auf

bestimmte Videomonitore, das Starten von vorkonfigurierten Sequenzen oder das Versenden SNMP-Events sein.
Darüber hinaus stellt **vimacc** sicher, dass alle erkannten Ereignisse und alle durchgeführten Aktionen kontextbezogen protokolliert werden. Eine kontextbezogene Dokumentation bedeutet in diesem Zusammenhang, dass die zu einem bestimmten Ereignis gehörenden Protokollmeldungen des Systems jederzeit abgerufen werden können, so dass eine lückenlose Verfolgung aller automatisch durchgeführten oder von einem Benutzer initiierten Aktionen möglich ist. **vimacc** ist dadurch in der Lage, ein Alarm-Management vollständig innerhalb des **vimacc** Teilsegmentes durchzuführen.

Darüber hinaus gibt es Programme zur Erledigung folgender Aufgaben:

- Peripherieverwaltung,
- Benutzer- und Rechteverwaltung
- Ansicht und Filterung von Reporting-Daten

Ein unbeschränktes Mehr-Augen-Prinzip kann zusätzlich zur Verschlüsselung der Streams, für den Zugriff auf einzelne Programmfunktionen und auf das Videomaterial konfiguriert werden und verbessert somit den Schutz der Daten.

Die Authentifizierung von Benutzern eines **vimacc**-Systems kann auf zwei verschiedene Arten erfolgen.

1. Über die integrierte Benutzerverwaltung, oder
2. Über die Anbindung an bestehende Verzeichnisdienste (z.B. Active Directory)

Die Benutzerverwaltung von **vimacc** basiert ähnlich wie ein AD auf Berechtigungsprofilen in Form von sogenannten Security-Tokens.
Die Feature-Listen sind signierte Klartextlisten, in denen die nutzbaren Funktionen aufgelistet werden, die in einer Anwendung von einem Benutzer auf einem bestimmten Rechner genutzt werden können.
**vimacc** stellt die Authentizität einer Feature-Liste über die Prüfung der Signatur des entsprechenden Administrators sicher. In einer vertrauenswürdigen Infrastruktur wie z.B. einem Active Directory können dort authentifizierte Benutzer via SingleSignOn direkt angemeldet werden.
Die vom Hersteller signierte Feature-Liste kann funktionale Einschränkungen enthalten, die die Konfigurationsmöglichkeiten des Videosystem-Administrators auf Kundenseite einschränken.

In als „sicher“ definierten Systemen werden Restriktionen vom Hersteller konfiguriert und ausgeliefert, die auf Betreiberseite nicht geändert werden können, um eine Konformität mit dieser Zertifizierung sicher zu stellen.

Die nicht zur Verfügung stehenden Funktionen sind im Kapitel *„Ausschlüsse und Restriktionen in Bezug auf den Begutachtungsgegenstand“* im Detail beschrieben.

## *Ausschlüsse und Restriktionen in Bezug auf den Begutachtungsgegenstand*

Ausschlüsse und Restriktionen im Sinne der Zertifizierung wurden z.B. für Kommunikationsverbindungen definiert, die aufgrund von Einschränkungen externer Systeme, nicht verschlüsselt betrieben werden können. Weiterhin sind Funktionen deaktiviert, die nach deutschem Datenschutzrecht nicht pauschal und ohne Einzelfallprüfung benutzt werden dürfen.

Es gelten folgende Einschränkungen:

1. Die Ende-zu-Ende-Verschlüsselung ist generell aktiviert und kann vom Administrator des Systems nicht abgeschaltet werden.
2. Die interne Kommunikation erfolgt ausschließlich verschlüsselt.
3. Audio-Streams können im System nicht aktiviert werden.
4. Der interne http-Server ist abgeschaltet und nicht Gegenstand der Zertifizierung.
5. Der interne RTSP-Server ist abgeschaltet und nicht Gegenstand der Zertifizierung.
6. Der vimaccFTP-Uploader ist abgeschaltet und nicht Gegenstand der Zertifizierung.
7. Die Kennwortrichtlinien sind gemäß BSI-Richtlinien gesetzt und können nicht geändert oder abgeschaltet werden. Längere Kennworte können jedoch definiert werden.
8. Ein Export kann nur verschlüsselt und mit Kennworten nach Komplexitätsrichtlinien erfolgen.
9. Das vimacc Control-Interface darf nicht im Modus für vollständigen Systemzugriff „VIMACC_CONTROL_INTERFACE_ALL=true“ betrieben werden.
10. Das Modul „Nummerschilderkennung“ ist ein Fremdprodukt. Es gehört nicht zum Gegenstand der Zertifizierung und ist abgeschaltet.

# D. Tools, die zur Herstellung des IT-Produktes verwendet wurden

Bei der Entwicklung kamen folgende Tools zum Einsatz:

- Microsoft Visual Studio
- SubVersion
- Jenkins
- BugZilla
- QT-Framework
- FFMPEG
- Open-SSL
- OpenCV

In der Testumgebung kamen folgende Tools zum Einsatz:

- Microsoft Server 2008/2012/2016
- Microsoft Windows XP, 7, 8.1, 10
- Linux Open Suse
- Suse Linux Enterprise SLED, SLES
- CentOS
- Kameras von verschiedenen Herstellern

# D. Zweck und Einsatzbereich des Begutachtungsgegenstandes

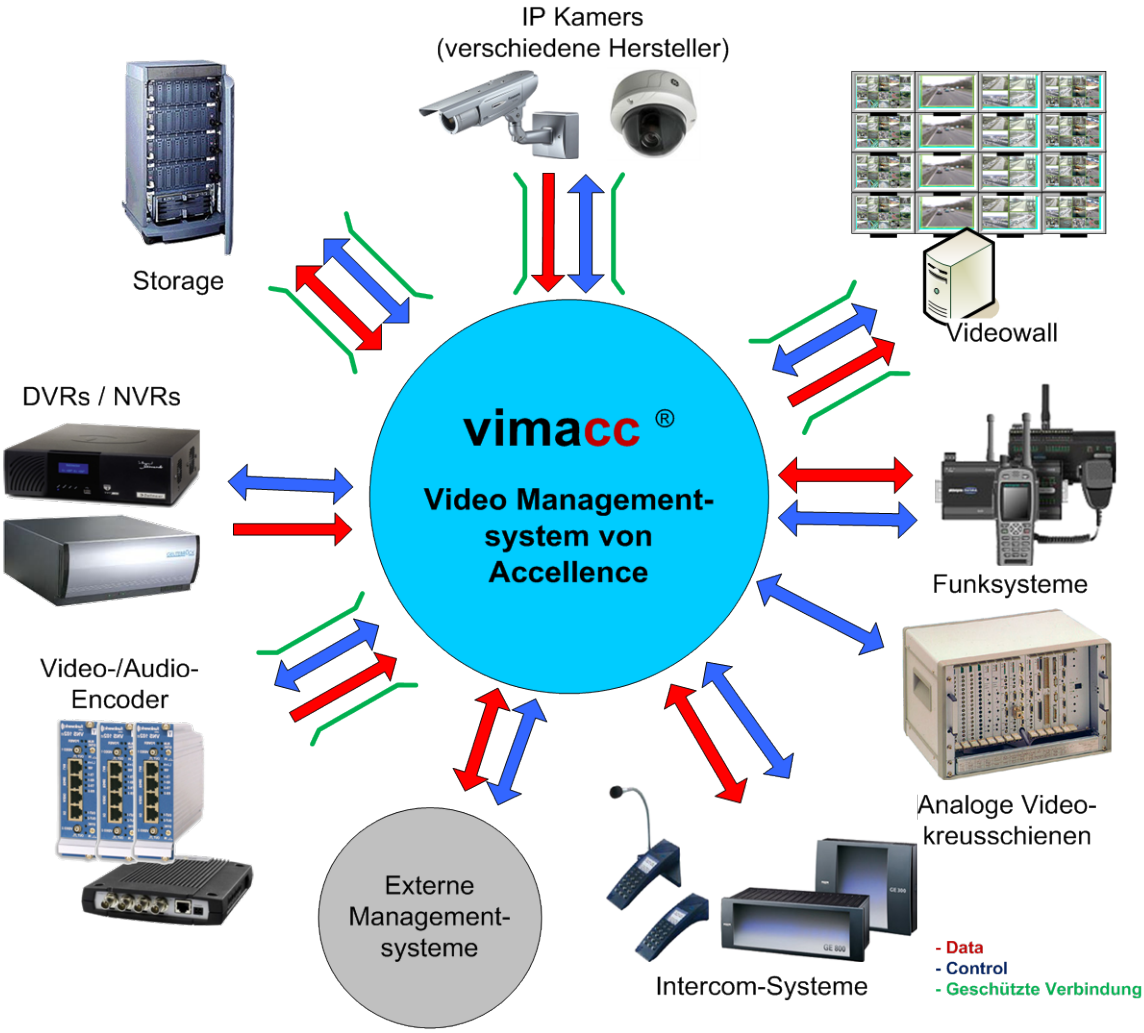
Einsatzzweck der Software ist die optisch-elektronische Überwachung von Räumen bzw. Bereichen. Diese kann wiederum für verschiedene Zwecke erfolgen. In vielen Fällen wird dies zur Wahrnehmung des Hausrechts geschehen. Dass die Software von der jeweils verantwortlichen Stelle in zulässiger Weise und für zulässige Zwecke eingesetzt wird, liegt allein im Verantwortungsbereich der verantwortlichen Stelle, also des Kunden des Produktherstellers. Festzustellen ist jedoch, dass ein rechtskonformer Einsatz mit dem Produkt in jedem Fall grundsätzlich möglich ist.
Bei Abweichungen des erforderlichen Funktionsumfanges von den gesetzten Restriktionen, ist eine detaillierte datenschutzrechtliche Prüfung auf Betreiberseite notwendig.

Die Struktur und die Komplexität der für den Einsatz von **vimacc** in Frage kommenden Zielsysteme können sehr unterschiedlich ausfallen. Das Spektrum reicht von sehr einfachen Systemen, die z.B. wenige Videokameras zur Beobachtung an eine zentrale Workstation (PC-Arbeitsplatz) anbinden, bis hin zu einer komplexen Topologie, bestehend aus verschiedenen unabhängigen Schutzobjekten, Standorten mit Unterzentralen und Zentralen, wie z.B. bei

einem U-Bahn-Verkehrsbetrieb, der aus vielen U-Bahn-Linien, mit vielen Teilsegmenten, ggf. Teilsegmentszentralen und Hauptzentralen besteht.
Der typische Aufbau von Teilsegmenten, in denen **vimacc** zum Einsatz kommen kann, umfasst die zu integrierende digitale bzw. analoge Videotechnik, ggf. Streaming-Server bzw. digitale Videorekorder für die Video-Stream-Aufzeichnung und ggf. Leitstandtechnik für die segmentspezifischen Überwachungsaufgaben.
Der Zertifizierungsgegenstand wird für Zwecke der Veranschaulichung und Verstehbarkeit nachfolgen anhand eines fiktiven Anwendungsbeispiels aus der Praxis erläutert.

*Beispielszenario*: Die Firma A-GmbH möchte die Außenanlagen ihres Standortes zum Zwecke des Objektschutzes überwachen. Dabei kommt **vimacc** zum Einsatz. Angeschlossen werden mehrere Kameras, die entsprechende Videoquellen darstellen. Alle Videoquellen werden in einer Überwachungszentrale zusammengeführt und dort auf einer Videowand dargestellt. Eine permanente detaillierte Beobachtung aller Bereiche ist nicht nötig; ebenso kann eine andauernde Aufzeichnung entfallen. Somit werden Alarme in Form von Bewegungserkennung in den verschiedenen Bereichen definiert. Sobald in diesen Bereichen eine Bewegung erkannt wird, zeichnet das System entsprechend den Einstellungen in einem bestimmten Zeitraum auf und gibt eine Alarmmeldung aus, so dass sich ein Beobachter die Aufzeichnung ansehen und ggf. Maßnahmen einleiten kann. Die Alarmmeldung wird quittiert und der Abschnitt wird gem. den Vorgaben des Unternehmens archiviert. In einer verschärften Form wird definiert, dass das Ansehen der Alarminformationen (und der damit verbundenen Aufzeichnung) nur durch ein Vier-Augen-Prinzip geschehen darf, d. h. nur bei Anwesenheit einer zweiten Person möglich ist.

# E. Datenflusses



# E. Zusammenfassung der Prüfergebnisse

Mit **vimacc** bietet der Hersteller des Produkts eine datenschutzfreundliche Video-Management-Software. Alle Daten, die von einer Videokameraausrüstung gesammelt werden, werden in der Kamera selbst (den Einsatz geeigneter Kameras vorausgesetzt) verschlüsselt. Die Übertragung von Videodaten ist während des Transports verschlüsselt. Die Daten werden auf dem Server ebenfalls ausschließlich verschlüsselt gespeichert und können nur von einem Benutzer entschlüsselt werden, der Zugriff auf einen Hardware-Dongle hat, der den privaten Schlüssel zum Entschlüsseln der Daten enthält.

**vimacc** bietet eine umfassende Möglichkeit, Benutzer und Zugriffsrechte für Benutzer zu verwalten.

Eine weitere positive Tatsache ist, dass das Produkt datenschutzfreundliche Optionen bietet, wie z. B. das Verpixeln von Bereichen, die Teil einer Videoaufzeichnung sind.

Das Produkt erleichtert eine datenschutzkonforme Nutzung der Videoüberwachung, die mit Hilfe des Zertifizierungsgegenstands durchgeführt wird. Im Vorfeld jedoch muss die verantwortliche Stelle prüfen, ob der Betrieb einer Videoüberwachung im konkreten Fall zulässig ist..

Accellence Technologies informiert seine Kunden mittels eines Datenschutz-Hinweisblattes über relevante Datenschutzaspekte. Dieses Hinweisblatt stellt den Nutzern von **vimacc** auch eine Checkliste zur Verfügung, die sie bei der Einsatzplanung für ein Videoüberwachungssystem unterstützen soll.

Schließlich ist anzumerken, dass Accellence Technologies ein spezifisches Lizenzmodell für **vimacc** anbietet, das auf die anwendbaren Anforderungen an das Datenschutzgütesiegel zugeschnitten ist und dafür sorgt, dass das Produkt unter den bereits oben erwähnten Einschränkungen läuft. Die einsetzende Stelle und die Benutzer von **vimacc** können die implementierte Konfiguration (Lizenz-Features) nicht ändern.

Im Hinblick auf die grundsätzliche Installation einer optisch-elektronischen Überwachung gelten nach § 20 Abs. 1 LDSG SH insoweit keine anderen Vorgaben als bei § 6b BDSG. Auch hier kann die Videoüberwachung zur Erfüllung der Aufgaben der öffentlichen Stelle oder zur Wahrnehmung des Hausrechts zulässig sein. Und wie § 6b BDSG ist auch hier eine Interessenabwägung mit den Belangen der Betroffenen vorzunehmen. Nach § 20 Abs. 2 LDSG SH ist wie bei § 6b BDSG auch eine Kenntlichmachung der Videoüberwachung erforderlich. Auch die Regelungen zur Speicherung und weiteren Verarbeitung der Daten in § 20 Abs. 3 LDSG SH sind nahezu identisch mit § 6b Abs. 3 BDSG.

Die Zuordnung zu einer Person und die damit einhergehende Benachrichtigungspflicht ergibt sich aus § 20 Abs. 4 LDSG SH. Auch insoweit besteht eine interessengleiche Regelung wie in § 6b Abs. 4 BDSG.

Und schließlich sind auch die Regelungen zur Löschung von Daten (§ 20 Abs. 5 LDSG SH und § 6b Abs. 5 BDSG) gleich.

Ob diese Voraussetzungen im Einzelnen vorliegen, liegt stets im Verantwortungsbereich der einsetzenden Stelle und ist durch diese vor jedem Einsatz zu prüfen. Im Hinblick auf die vorzunehmende Interessenabwägung, kann die in dem Zertifizierungsgegenstand verwendete datenschutzfreundliche Technologie, die Zulässigkeit des jeweiligen Vorhabens fördern.

Festzustellen ist jedenfalls, dass ein datenschutzkonformer Einsatz unter Einhaltung der jeweils geltenden Rechtsgrundlagen grundsätzlich möglich ist.

| **Anforderung nach Katalog oder sonstigen Rechtsnormen** | **Bewertung** | **Kommentare** |
|---|---|---|
| **Komplex 1:** | | |
| 1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit | vorbildlich | |
| 1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung) | vorbildlich | |
| 1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung) | vorbildlich | |
| 1.4 Datenschutz-Schutzziel: Intervenierbarkeit | vorbildlich | |
| 1.5 Anpassung des IT-Produkts | vorbildlich | |
| 1.6 Privacy by Default | vorbildlich | |
| 1.7 Sonstige Anforderungen | entfällt | |
| | | |
| **Komplex 2:** | | |
| 2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten | adäquat | |
| 2.1.2 Einwilligung des Betroffenen | entfällt | |
| 2.1.3.1 Vorschriften über die Datenerhebung | entfällt | |
| 2.1.3.2 Vorschriften über die Übermittlung | entfällt | |
| 2.1.3.3 Löschung nach Wegfall des Erfordernisses | entfällt | |
| 2.2.1 Zweckbindung und Zweckänderung | entfällt | |
| 2.2.2 Erleichterung der Umsetzung des Trennungsgebotes | entfällt | |

| Anforderung nach Katalog oder sonstigen Rechtsnormen | Bewertung | Kommentare |
|---|---|---|
| 2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG) | entfällt | - |
| 2.3 Datenverarbeitung im Auftrag | entfällt | - |
| 2.4.1 gemeinsame Verfahren/Abrufverfahren | entfällt | - |
| 2.4.2 Trennung der Verantwortlichkeiten | entfällt | - |
| 2.4.3 Veröffentlichungen im Internet | entfällt | |
| 2.4.4 Weitere besondere technische Verfahren | entfällt | |
| 2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens | entfällt | |
| | | |
| **Komplex 3:** | | |
| 3.1.1. Physikalische Sicherung | entfällt | |
| 3.1.2 Authentisierung | adäquat | |
| 3.1.3 Autorisierung | adäquat | |
| 3.1.4 Protokollierung | adäquat | |
| 3.1.5 Verschlüsselung und Signatur | vorbildlich | |
| 3.1.6 Pseudonymisieren | entfällt | |
| 3.1.7 Anonymisieren | entfällt | |
| 3.2.1.1 Verfügbarkeit | vorbildlich | |
| 3.2.1.2 Integrität | vorbildlich | |
| 3.2.1.3 Vertraulichkeit | vorbildlich | |
| 3.2.1.4 Nicht-Verkettbarkeit | vorbildlich | |
| 3.2.1.5 Transparenz | adäquat | |
| 3.2.1.6 Intervenierbarkeit | entfällt | |
| 3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen | adäquat | |
| 3.2.1.8 Test und Freigabe | adäquat | |
| 3.2.2 Erleichterung der Vorabkontrolle | adäquat | |
| 3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses | adäquat | |
| 3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten | entfällt | |
| 3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten | adäquat | |
| 3.3.1 Verschlüsselung | vorbildlich | |
| 3.3.2 Anonymisierung oder Pseudonymisierung | adäquat | |

| Anforderung nach Katalog oder sonstigen Rechtsnormen | Bewertung | Kommentare |
|---|---|---|
| 3.3.3.1 Mobile Datenverarbeitungssysteme | entfällt | |
| 3.3.3.2 Video-Überwachung und –Aufzeichnung | entfällt | |
| 3.3.3.3 Automatisierte Einzelentscheidungen | entfällt | |
| 3.3.3.4 Veröffentlichungen im Internet | entfällt | |
| 3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren | adäquat | |
| 3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung | entfällt | |
| 3.6 Sonstige Anforderungen | entfällt | |
| | | |
| **Komplex 4:** | | |
| 4.1 Aufklärung und Benachrichtigung | adäquat | |
| 4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten | adäquat | |
| 4.3 Auskunft | adäquat | |
| 4.4.1 Berichtigung | adäquat | |
| 4.4.2 Vollständige Löschung | adäquat | |
| 4.4.3 Sperrung | adäquat | |
| 4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung | adäquat | |
| 4.3.5 Gegendarstellung | adäquat | |
| 4.5 Sonstige Anforderungen | entfällt | |

Zum Komplex 4 kann festgestellt werden, dass ein Betroffener sein Auskunftsrecht jederzeit gegenüber der verantwortlichen Stelle geltend machen kann. Verantwortliche Stelle für die Datenverarbeitung ist der jeweilige Kunde des Produktherstellers. Ob die verantwortliche Stelle die Betroffenenrechte in rechtlich zulässiger Weise gewährleistet, liegt nicht im Verantwortungsbereich des Produktherstellers. Auch hier ist wiederum entscheidend, dass das Produkt grundsätzlich in datenschutzrechtlich zulässiger Weise eingesetzt werden kann. Auch das ist hier der Fall.

Insgesamt kann festgestellt werden, dass das Produkt **vimacc 2.2** die Voraussetzungen für den Erhalt eines Gütesiegels für IT Produkte erfüllt. Beim Einsatz des Produktes durch öffentliche Stellen des Landes Schleswig-Holstein können alle datenschutzrechtlichen Vorschriften eingehalten werden.

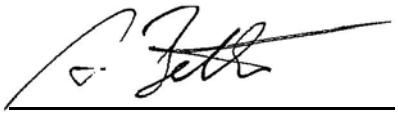
# H. Beschreibung, wie das Produkt den Datenschutz fördert

Durch die Unterstützung einer Ende-zu-Ende-Verschlüsselung werden in **vimacc** die Videodaten,beim Einsatz geeigneter Kameras, bereits in der Kamera verschlüsselt und durch den Einsatz von Hardware-Dongles nur den Personen zur Verfügung gestellt, die neben dem Dongle auch über die PIN für den Dongle verfügen und berechtigte Benutzer im System sind.
Zudem ist es möglich ein unbeschränktes Mehr-Augen-Prinzip umzusetzen. Gemeint ist damit, dass sich mehrere Personen mit BSI-konformen Kennworten am System authentifizieren müssen, um eine bestimmte Funktion auszuführen oder einen Video-Stream aufschalten zu können. Für datenschutzrelevante Funktionen wird ein Mehr-Augen-Zugriff empfohlen.

**vimacc** besitzt spezielle Eingabefelder, in denen der Betreiber die datenschutzrelevanten Informationen zum Einsatzzweck der Kamera eingeben kann.
Diese Informationen stehen bei einer Revision oder Überprüfung des Systems einem Auditor zur Verfügung, der die Aktualität des Einsatzes der Kameras adäquat prüfen kann.
Weiterhin bietet **vimacc** die Möglichkeiten eine Bestandsdokumentation mit Bildern aller Kamera-Streams inkl. der konfigurierten verpixelten Flächen als PDF-Datei zu erzeugen. Mit Hilfe dieses Dokumentes kann jederzeit sehr schnell die korrekte Konfiguration des Gesamtsystems geprüft und ggf. an geänderte datenschutzrechtliche Anforderungen angepasst werden.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 09.02.20167



Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (technisch)

Flensburg, den 09.02.2017

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für IT-Produkte (rechtlich)