

Gutachten zur Erteilung eines Datenschutz- Gütesiegels für die Produkte

***DIBIKO - Digitale Bildintegration für Kommunen
mit Fotokabine VC 100***

sowie

DIBIKO Small Business (ohne Fotokabine)

im Auftrag der Firmen Vending Concept - Forum GmbH - Roa Consult

datenschutz nord GmbH
Mai 2007

Inhaltsverzeichnis

1.	Stellenwert des Datenschutzaudits _____	3
2.	Angaben zum Gutachten _____	3
2.1	Antragsteller _____	3
2.2	Sachverständige _____	3
2.3	Prüfzeitraum und -verfahren _____	3
3.	Gegenstand des Audits _____	4
3.1	Produkte _____	4
3.2	Einsatzumgebung _____	8
3.3	Schnittstellen _____	9
4.	Gesetzliche Rahmenbedingungen _____	10
5.	Anforderungskatalog _____	10
6.	Bewertung der besonderen Eigenschaften _____	11
6.1	Bewertung des Produkts _____	11
6.2	Datenschutzfördernde Merkmale _____	15
6.3	Gesamtbewertung _____	16
	Anlage 1: Protokollreport Münzen (Beispiel) _____	17
	Anlage 2: Protokollreport der dBase-Datenbank (Beispiel) _____	18
	Anlage 3: Mustervertrag zu Support und Auftragsdatenverarbeitung _____	19

1. Stellenwert des Datenschutzaudits

Mit dem vorliegenden Gutachten wird die datenschutzrechtliche Auditierung der Produkte DIBIKO - Digitale Bildintegration für Kommunen mit Fotokabine VC 100 sowie der Version ohne Fotokabine, „DIBIKO Small Business“ (nachfolgend nur DIBIKO, Anwendung oder Produkt) dokumentiert, mit der die datenschutz nord GmbH von den Firmen Vending Concept, Forum GmbH und Roa Consult im Februar 2007 beauftragt wurde.

Rechtliche Basis des Gütesiegels in Schleswig-Holstein ist § 4 Absatz 2 des Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH), der von öffentlichen Stellen des Landes Schleswig-Holstein fordert, vorrangig solche Produkte einzusetzen, die mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar sind. Das zu auditierende Produkt muss daher auch zur Nutzung durch öffentliche Stellen des Landes Schleswig-Holstein geeignet sein (§ 1 Abs. 2 DSAVO). Für die Produkt-Eignung reicht es insoweit aus, dass eine öffentliche Stelle das Produkt selbst betreiben könnte.

Die vorliegend zu begutachtenden Produkte „könnten“ nicht nur von Kommunen in Schleswig-Holstein betrieben werden, sondern sind - weit über diese Anforderung hinausgehend - speziell dafür entwickelt worden, von Kommunen bzw. deren Meldeämtern eingesetzt zu werden, um den Prozess der Ausweiserstellung zu vereinfachen, indem Medienbrüche aufgehoben werden (ausführlicher dazu in der Produktbeschreibung, vgl. Ziff. 3.1)

Durch das vorliegende Gutachten wird geprüft, inwieweit die Produkte den Rechtsvorschriften über den Datenschutz und die Datensicherheit entsprechen. Hierfür wird zunächst in Kapitel 3 das Produkt in der Hauptversion sowie in der „kleineren“ Variante (Small Business) beschrieben, anschließend in Kapitel 4 die rechtlichen Grundlagen bestimmt sowie in Kap. 5 ein Anforderungsprofil als Soll-Vorstellung aus den Rechtsnormen abgeleitet, bevor anschließend in Kapitel 6 auf Basis der Produktbeschreibungen der Ist-Zustand der tatsächlichen Umsetzung festgestellt und bewertet wird.

2. Angaben zum Gutachten

2.1 Antragsteller

Antragsteller dieses Gutachtens sind die Firmen Vending Concept, die Forum GmbH sowie die Roa Consult, Roland Appel. Ansprechpartner sind Herr Roland Appel, Herr Andreas Schramm sowie Herr Marcel Moser.

2.2 Sachverständige

Sachverständige dieses Gutachtens ist die datenschutz nord GmbH, Barkhausenstr. 2, 27568 Bremerhaven. Ansprechpartner sind Herr Oliver Stutz und Dr. Uwe Schläger.

2.3 Prüfzeitraum und -verfahren

Die Begutachtung der Produkte erstreckte sich auf den Zeitraum von März bis April 2007 und beinhaltete neben der konzeptionellen Analyse der zur Verfügung

gestellten Unterlagen insbesondere auch eine Begutachtung und Tests des Produkts vor Ort (DIBIKO-Fotokabinen Installation im Rathaus Berlin-Reinickendorf).

3. Gegenstand des Audits

3.1 Produkte

Begutachtet wurden die Produkt DIBIKO - Digitale Bildintegration für Kommunen mit Fotokabine VC 100 sowie DIBIKO Small Business.

3.1.1 Produktumfang - DIBIKO mit Fotokabine VC 100

Bei dem Produkt handelt es sich um eine Kombination aus einer (herkömmlichen) digitalen Fotokabine mit integrierter biometrischer Bildbearbeitung. Es setzt sich aus folgenden Komponenten zusammen:

- Fotokabine (Breite 1450 mm, Höhe 2100mm, Tiefe 750 mm).



Bei der Fotokabine handelt es sich um ein geschlossenes System mit physischer Sicherung des Rechners und aller Komponenten (V2A-Stahl), diese sind mit einem Panzerschloss mit 6-facher Verriegelung vor dem Zugriff Unberechtigter bzw. vor Vandalismus geschützt. Das (ebenfalls in die physische Sicherung der Komponenten einbezogene) Ethernetkabel ist zusätzlich stahlummantelt. Das System ist stets in den Räumen der Meldebehörde installiert und somit auch nur während der allgemeinen Öffnungszeiten zugänglich. Die Komponenten umfassen:

- Fotokabinen-(DIBIKO-)PC mit CPU 2,8 MHz, 512 MB RAM, Ethernetschnittstelle (Netzwerkkarte), Betriebssystem: Win XP Professional
- Digitalkamera Canon Powershot A 620 (Anschluss über USB-Port)
- Proprietär installierte Software:
 - DIBIKO-Software

- Viisage “Face Tools” (Fa. Viisage, Bochum)
- dBase-Datenbank
- Thermosublimationsdrucker zum Ausdruck der Ursprungsbilder und der Einwilligungserklärung

3.1.2 Funktionsweise und Umfang der Datenverarbeitung

Das System dient der Erstellung vorgabenkonformer biometrischer Passbilder zur Verwendung in Personaldokumenten (Reisepässe, Personalausweise, Führerscheine) .

Der Nutzer wird unmittelbar nach dem Geldeinwurf auf dem Touchscreen zunächst nach der von ihm favorisierten Bediensprache gefragt (derzeit sind 6 Sprachen verfügbar). Nach Auswahl der gewünschten Sprache wird ihm in dieser Sprache eine Einwilligungserklärung präsentiert, die mit „Ja“ oder „Nein“ beantwortet werden kann (zum Wortlaut der Einwilligungserklärung vgl. unten Ziff. A 3).

Nach Bestätigen der Einwilligungserklärung über den Button auf dem Touchscreen werden über die Digitalkamera drei Portraitaufnahmen angefertigt. Diese bearbeitet die Viisage-Software anschließend nach den biometrischen Vorgaben der internationalen ICAO-Norm (International Civil Aviation Organization) und speichert zu jedem Ursprungsbild maximal ein weiteres als biometrisch verwendbares Bild (JPEG-Datei) auf der Festplatte des DIBIKO-PC (durch die Bearbeitung wird z.B. aus dem aufgenommenen Bild ein bestimmter Teilbereich ausgeschnitten, der für den Ausweis verwendet werden kann). Bei Geeignetheit der Bilder - wenn also aus jedem aufgenommenen Foto auch ein biometrisch taugliches erstellt werden kann - können somit maximal 6 Bilder gespeichert werden. In der Regel sind jedoch nur ein bis zwei Fotos auch als biometrietauglich verwendbar, dann werden entsprechend nur 4 oder 5 Fotos (Dateien) gespeichert. Die gespeicherten Fotos werden jeweils mit einer 10-stelligen Schlüsselzahl versehen, die über einen Zufallszahlen-Generator erzeugt wird und die - je nach Bedarf der Kommune - entweder vollständig zufällig ist oder in den ersten 5 Stellen die örtliche Postleitzahl enthält, in den übrigen 5 Stellen dann zufällig ist. Als Zufallszahlengenerator wird die C++-Funktion „randomize“¹ verwendet (die Funktion randomize wird bereits beim Starten der Fotokabine aufgerufen). Der Zufallszahl der biometrietauglichen Fotos wird automatisch das Kürzel ICAO vorangestellt.

In der dBase-Datenbank werden die Erstellungsdaten der Bilder (Protokoll- bzw. Reportdaten) gespeichert. Hierbei handelt es sich um folgende Angaben

- fortlaufende Nummer
- Datum
- Uhrzeit
- zu zahlender Betrag (in Euro)

¹rand verwendet ein multiplikatives Kongruenzverfahren (Multiplikation mit anschließender Modulo-Operation), um Pseudo-Zufallszahlen im Bereich von 0 bis RAND_MAX zu erzeugen. Die Periode des Zufallszahlengenerators beträgt pow(2,32) = 4294967296. rand liefert die Pseudo-Zufallszahl zurück.

- gezahlter Betrag
- Druckerstatus
- MwSt.
- Währung
- Münzen (Münzart)
- Flag ICAO-konform

Der in der bisherigen Abrechnungsperiode kumuliert gezahlte Betrag wird ebenfalls erfasst (vgl. hierzu die Protokollreports in den **Anlagen 1 und 2**).

Die Ursprungsbilder werden gemeinsam mit der Einwilligungserklärung über einen Thermosublimationsdrucker wie in einer herkömmlichen Fotokabine ausgedruckt, so dass sie als herkömmliches Passfoto mitgenommen werden können - diese Funktion dient sowohl als „Add-On“, um den Kunden einen zusätzlichen Wert zu bieten (über die für sie nicht „greifbare“ biometrische Bilddatei hinaus), als auch dem Zweck, den Nutzern die Einwilligungserklärung in schriftlicher Form (auf Papier) zur Verfügung stellen zu können.

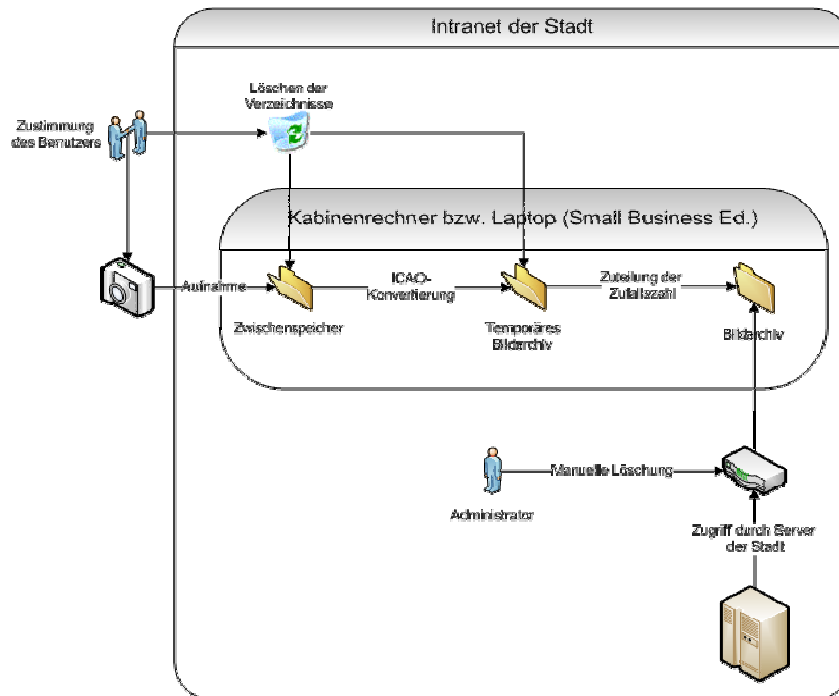
Die Art und Weise des (behördlichen) Abrufs des Bildes ist variabel: Da der Fotokabinen-PC stets Bestandteil der Netzinfrastruktur der Kommune ist, wird dieser im kommunalen Netz in der Regel als separates Laufwerk angesprochen. Über die Meldesoftware (MESO o.ä.) kann die Quelle, aus der das Bild für den biometrischen Reisepass importiert wird, frei bestimmt werden. Gewöhnlich ist dies ein Scanner im Raum des Sachbearbeiters - bei Einsatz von DIBIKO wird dann als Quelle der Fotokabinen-PC bestimmt. Um das Bild importieren zu können, ist die Eingabe der vom Bürger vorgelegten Zufallszahl erforderlich, nur so kann das Bild zugeordnet werden.

Auf Wunsch der Kommune können die erzeugten Bilder auch auf einen separaten Server im Netzwerk exportiert werden, von dem dann die Bilder in die Meldebehörden-Software integriert werden, diese Funktion kann über die DIBIKO-Software implementiert werden.

Sobald das taugliche Bild vom Sachbearbeiter über die entsprechende Meldebehörden-Software abgerufen wird, werden alle auf der Festplatte des Fotokabinen-PC befindlichen Bilder (sowohl die Ursprungsbilder, als auch die Biometriebilder) gelöscht. Die gespeicherten Bilder bleiben somit auf dem Fotokabinen-PC gespeichert, bis der Sachbearbeiter das Bild (unter Vorlage der Zufallszahl) abrufen, maximal jedoch für einen Zeitraum von 3 Monaten (vgl. Einwilligungserklärung unten Ziff. A3).

Nach Übernahme des Bildes in die Meldesoftware, wird das Bild nochmals über die Schnittstelle zum Bundesdruckereiverfahren DIGANT auf die Biometrietauglichkeit geprüft, dieser letzte Schritt betrifft nicht mehr das hier begutachtete Produkt.

3.1.3 Datenflussmodell



3.1.4 Produktumfang DIBIKO Small Business

Wie aus der Produktbezeichnung bereits erkennbar, umfasst die „kleinere“ Variante des Produkts keine Fotokabine. Stattdessen setzt sich das Produkt aus folgenden Komponenten zusammen:

- Laptop 2 GHz, 512 MB RAM, Windows XP Professional, DIBIKO-Software und dBase-Datenbank vorinstalliert, Maus, Ethernetkabel
- Digitalkamera Canon Powershot A 620 mit Stativ
- Thermosublimationsdrucker (Epson)
- Transportkoffer für die gesamte Ausstattung



3.1.5 Funktionsweise DIBIKO Small Business

Die Funktionsweise entspricht der bereits zur Fotokabinen-Version dargestellten mit der Besonderheit, dass die Small Business-Version in den Räumen der Sachbearbeiter aufgestellt wird (Herstellerempfehlung bzw. –vorgabe) und nur von diesen bedient wird. Die Small Business Version enthält keine zahlungsrelevanten Vorrichtungen und keine Abrechnungsfunktion.

3.1.6 Benutzerverwaltung und Berechtigungskonzept

Da der Fotokabinen-PC mit Integration in das Netzwerk der Behörde bzw. der Kommune stets Bestandteil dieses Netzwerks wird, obliegt die Einrichtung der Benutzer und die Erstellung eines Berechtigungskonzepts bzw. die Erreckung des bestehenden behördlichen Berechtigungskonzepts auf das betreffende Laufwerk allein dem zuständigen Netzwerk-Administrator. Der Zugriff auf die Bilder erfolgt behördlicherseits somit nur durch die berechtigten Nutzer. Die Herstellerempfehlung sieht hierzu vor, die Berechtigungen an diejenigen zu koppeln, die für die Nutzung der jeweiligen Behördensoftware (z.B. MESO) gelten.

Auf der Grundlage des mit der jeweiligen Kommune bei Einrichtung der Fotokabine abzuschließenden Support-Vertrages haben auch Mitarbeiter des Herstellers Zugriff auf die Bilddaten. Der Hersteller wird im Rahmen dieser Tätigkeit als Auftragsdatenverarbeiter für die Kommune tätig und unterliegt damit entsprechend den landesrechtlichen Vorgaben zur Auftragsdatenverarbeitung den Regelungen des schriftlichen Vertrages zur Auftragsdatenverarbeitung. Ein Muster des vom Hersteller verwendeten Support- und Auftragsdatenverarbeitungsvertrages liegt als **Anlage 3** bei.

3.1.7 Produktdokumentation

Für das Produkt DIBIKO liegt folgende Produktdokumentation vor:

- DIBIKO Produktbeschreibung
- DIBIKO Datenschutz- und -sicherheitskonzept
- Garantiebedingungen mit Betriebsanleitung und Herstellerempfehlungen zur Einsatzumgebung

3.2 Einsatzumgebung

Die IT-Sicherheit von DIBIKO ist aufgrund der Einbindung in die jeweilige Netzinfrastruktur der Kommune bzw. des betreffenden Meldeamtes wesentlich von den dortigen Sicherheitsmechanismen abhängig.

Der Hersteller hat keinen direkten Einfluss auf die Einrichtung von Datensicherheitsmaßnahmen im betreffenden kommunalen Netzwerk bzw. im Netzwerk der jeweiligen Behörde. Gleichwohl werden sowohl im Datenschutz- und –sicherheitskonzept des Herstellers, als auch in den Herstellerempfehlungen (Bestandteil der Betriebsanleitung) an die Einsatzumgebung folgende Anforderungen gestellt:

- Räumliche Umgebung

Für die Aufstellung des DIBIKO Systems wird ein abgeschlossenes (Bürger-) Büro, vorausgesetzt, das ein unbefugtes Bedienen oder einen unberechtigten Zugang zu Hard- oder Software und insbesondere zu den Bilddaten ausschließt. Der Rechner soll außerhalb der Dienstzeiten verschlossen aufbewahrt werden (*gilt für DIBIKO Small Business*). DIBIKO darf nur von dafür autorisierten Personen bedient werden.

--- Netzwerkimtegration

Die elektronische Anbindung des DIBIKO Systems erfolgt über ein 100 MBit Ethernetkabel und Vergabe fester (interner) IP-Adresse mit Identifikation der MAC-Adresse des Systems. Der DIBIKO-PC darf weder unmittelbar noch mittelbar aus dem Internet erreichbar sein bzw. IP-Verbindungen nach außen aufbauen dürfen. Es wird empfohlen, darüber hinaus Passwörter zu vergeben, mit denen sich der DIBIKO-PC im Netzwerk der Kommune identifiziert. Eine drahtlose Anbindung z.B. über WLAN ist nicht hinreichend gegen unbefugtes Eindringen gesichert und darf nicht verwendet werden.

--- Firewall und Virenschutz

DIBIKO ist grundsätzlich nur in einer Hardwareumgebung zu betreiben und elektronisch zu verbinden, die ihrerseits durch Firewall oder Virens Scanner gegen Schadsoftware und fremde Datenzugriffe gesichert ist. Dritt-Software darf auf dem DIBIKO-PC bzw. –Laptop nicht installiert werden.

--- Berechtigungskonzept

Für das vom Hersteller und der Behörde gemeinsam definierte Austauschverzeichnis gelten grundsätzlich die gleichen Zugriffsberechtigungen und Sicherheitsbestimmungen, wie für die behördenintern genutzte Melde- und Ausweissoftware

--- Protokollierung

Zugriffe auf das Austauschverzeichnis und bzw. auf das Bildverzeichnis des Rechners von DIBIKO sind zu protokollieren.

--- Datensicherung

Das Austausch- bzw. Bildverzeichnis ist mit in das Datensicherungskonzept der Behörde zu integrieren, damit die Verfügbarkeit der Bilder auch bei unvorhergesehenen Ausfällen des Netzwerkes gewährleistet ist.

--- Löschrfristen

Die Bilddaten im Austauschverzeichnis sind nach spätestens drei Monaten zu löschen.

3.3 Schnittstellen

Außer den an einem „handelsüblichen“ PC befindlichen Hardware-Schnittstellen weist das DIBIKO-System keine weiteren Schnittstellen auf. Die DIBIKO-Software stellt die Bilder auf Dateisystemebene zur Verfügung und zwar, entsprechend der Einstellung, entweder in einem festgelegten Verzeichnis auf der lokalen Festplatte

des Fotokabinen-PC, oder - nach einem Export - auf einem (Server-)Verzeichnis eines ausgewählten Behörden-Servers im lokalen Netzwerk.

Eine Fernwartung erfolgt nicht, der unter Ziff. 3.1.4 beschriebene Support-Zugriff durch den Hersteller erfolgt stets lokal vor Ort.

4. Gesetzliche Rahmenbedingungen

Zentrale Rechtsgrundlage für die zuvor beschriebene Datenverarbeitung ist die Einwilligung der Betroffenen, deren Anforderungen sich nach demjenigen Landesdatenschutzgesetz richten, das für die betreffende Kommune gilt, in Schleswig-Holstein ist insoweit § 11 Abs. 1 Nr. 1 i.V.m. § 12 LDSG S-H einschlägig.

Als gesetzliche Rahmenbedingungen zur Erstellung gesetzestrunder Passbilder zur Verwendung in Reisepässen und Personalausweisen gelten die PassV 2004 (für Personalausweise), sowie die PassMustV und insbesondere deren Anlage 3 zu § 3 PassMustV, die im Detail die Anforderungen an das biometrische Bild beschreibt.

Die behördliche Verarbeitung der Lichtbilder im Zusammenhang mit der Passerstellung ist nicht mehr Gegenstand des Produkts, die Vorgaben des PaßG zur Datenverarbeitung zählen daher nicht zu den hier relevanten rechtlichen Rahmenbedingungen.

Bei den im DIBIKO-System gespeicherten Protokolldaten handelt es sich nicht um personenbezogene Daten, da in der dBase-Datenbank nicht die generierte Zufallsziffer, sondern lediglich eine fortlaufende Nummer gespeichert wird. Auf diese Weise ist kein Personenbezug herstellbar, selbst wenn die Bilddatei noch auf der Festplatte des DIBIKO-PC vorhanden ist. Aus diesem Grunde sind für die Protokolldaten keine datenschutzrechtlichen Vorgaben einschlägig.

5. Anforderungskatalog

Aus den in Kap. 4 aufgeführten rechtlichen Rahmenbedingungen ergibt sich für die Bilddaten ein konkretes Anforderungsprofil, welches wie folgt unterteilt werden kann:

Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

A1 Aussagefähige Produktbeschreibung

Liegt für DIBIKO eine aussagekräftige und aktuelle Produktbeschreibung vor, so dass Anwender – auch ohne Vorkenntnisse – die Applikation korrekt bedienen können?

A2 Datensparsamkeit, Verwendung von Pseudonymen

Werden bei der Verarbeitung der Bilddaten Prinzipien der Datensparsamkeit ausreichend berücksichtigt? Werden Pseudonyme verwendet?

Komplex 2: Zulässigkeit der Datenverarbeitung

A3 Zulässigkeit der Verarbeitung der Bilddaten

Werden die Bilddaten unter Beachtung der Einwilligungserklärung in zulässiger Weise erhoben, verarbeitet und gelöscht?

Komplex 3: Technisch-organisatorische Maßnahmen

- A4 Authentizität der Behörden-Nutzer
- A5 Authentizität des DIBIKO-PC
Existieren geeignete Mechanismen zur Authentisierung des DIBIKO-PC?
- A6 Vertraulichkeit der Daten
Werden die Bilddaten auf dem DIBIKO-PC vertraulich gespeichert?
- A7 Integrität der Daten
Ist die Integrität der auf dem DIBIKO-PC gespeicherten Daten sichergestellt?
Können Manipulationen nachträglich durch entsprechende Mechanismen erkannt werden?
- A8 Verfügbarkeit der Daten
Wird die Verfügbarkeit durch ausreichende Backup-Mechanismen sichergestellt?
- A9 Revisionsfähigkeit
Ist nachvollziehbar, zu welchem Zeitpunkt welche Daten gespeichert werden?

Komplex 4: Umsetzung der Betroffenenrechte

- A10 Können Auskunftersuchen von Nutzern bezüglich der Speicherung und Löschung der Bilddaten durch das Produkt angemessen unterstützt werden?

6. Bewertung der besonderen Eigenschaften

Die Bewertung der besonderen Eigenschaften des Produkts erfolgt in zwei Kapiteln. Zunächst erfolgt die Bewertung des Produkts für die Primär- und Sekundärdaten, anschließend die Bewertung der datenschutzfördernden Merkmale. Eine Zusammenfassung der Prüfergebnisse rundet dieses Kapitel ab.

Vorausgesetzt wird eine sichere Einsatzumgebung, wie sie in Kap. 3.2 als Herstellerempfehlung dargestellt wurde.

6.1 Bewertung des Produkts

In die Bewertung der Anwendung sind neben der konzeptionellen Analyse der zur Verfügung gestellten Unterlagen Tests und Begutachtungen eines installierten Systems vor Ort mit eingeflossen.

A1 Aussagefähige Produktunterlagen

Von den Antragstellern wurden folgende Produktunterlagen zur Verfügung gestellt:

- DIBIKO Produktbeschreibung VC 100
- DIBIKO Produktbeschreibung SMALL BUSINESS
- DIBIKO Datenschutz- und -sicherheitskonzept
- Garantiebedingungen mit Betriebsanleitung und Herstellerempfehlungen zur Einsatzumgebung

Die Unterlagen sind insgesamt verständlich und aussagekräftig; dies gilt insbesondere für das Datenschutz- und Sicherheitskonzept, in dem neben den technischen Rahmenbedingungen auch die Voraussetzungen für die Umsetzung der Betroffenenrechte durch vertraglich erforderliche Vereinbarungen mit den verantwortlichen Stellen erläutert werden.

A2 Datensparsamkeit, Verwendung von Pseudonymen

Das Produkt ist vollständig auf die Verwendung von Pseudonymen zugeschnitten: Bei den erzeugten Bilddaten handelt es sich, ohne dass hier auf weiterführende Fragen zum erforderlichen Zusatzwissen eingegangen werden muss, auch bei Verwendung von Zufallszahlen um zumindest personenbeziehbare und damit um personenbezogene Daten i.S.d. § 4 BDSG. Die Verwendung von Zufallszahlen als Dateibezeichnung und damit die Erstellung von pseudonymen Dateien erschwert jedoch die Möglichkeit des Personenbezuges in einem angemessenen Maß und kommt der Forderung des § 3a S. 2 BDSG bzw. § 4 Abs. 1 LDSG S-H in vollem Umfang nach.

A3 Zulässigkeit der Verarbeitung der Bilddaten

Zulässigkeit der Erhebung und Speicherung

Die Zulässigkeit der Verarbeitung der Bilddaten bestimmt sich nach der von den Nutzern erklärten Einwilligung, die vor der Bilddatenerzeugung präsentiert wird:

„Ihr Bild wird anonym und unter einem Zahlenschlüssel gespeichert, der nur Ihnen persönlich gehört. Bewahren Sie den Zahlenschlüssel sorgfältig auf. Legen Sie ihn mit Ihrem Passantrag bei den zuständigen Sachbearbeitern vor. Dieser kann Ihr Bild nur damit abrufen oder löschen. Das Bild wird ausschließlich für die Erstellung Ihres Passes verwendet. Eine anderweitige Nutzung ist ausgeschlossen. Die Speicherung erfolgt für einen Zeitraum von maximal 3 Monaten, d.h. wenn Sie das Bild bis zum Ablauf dieses Zeitraums nicht durch Beantragung eines Ausweisdokuments abgerufen haben, wird es automatisch gelöscht.

Wenn Sie mit dieser Datenverarbeitung einverstanden sind, drücken Sie „Ja“, ansonsten „Nein“

NEIN

JA

Die Anforderungen an eine wirksame Einwilligung richten sich in Schleswig-Holstein nach § 12 LDSG S-H. Danach bedarf die Einwilligung grundsätzlich der Schriftform (Abs. 1), wobei in Ausnahmefällen auch die elektronische Form möglich ist, wenn die Voraussetzungen nach § 12 Abs. 3 LDSG S-H eingehalten werden.

Da die Einwilligung hier, wie zuvor erläutert, durch Betätigen des Touchscreen-Buttons und damit elektronisch erklärt wird, müssen die weiteren Voraussetzungen des § 12 Abs. 3 LDSG S-H vorliegen, nämlich

- eine eindeutige und bewusste Handlung des Betroffenen
- die Sicherstellung der Unveränderbarkeit
- Klarheit über den Urheber

--- eine Protokollierung der Einwilligung bei der verarbeitenden Stelle

Indem der Nutzer zwischen der Zustimmung und der Ablehnung der Einwilligungserklärung klar wählen kann und auch keine Voreinstellung getroffen ist, liegt mit der Auswahl des Ja-Buttons eine eindeutige Handlung vor. Darüber hinaus ist die Einwilligungserklärung sowohl durch die Software fest vorgegeben, als auch durch den stets erfolgenden (Papier-)Ausdruck nicht mehr veränderbar. Aus der Erklärung wird auch hinreichend deutlich, dass speichernde Stelle und damit Urheber der Erklärung stets die Behörde vor Ort ist. Die Protokollierung erfolgt hier indirekt insoweit, als die Erzeugung und Speicherung der Bilddaten ohne vorherige Einwilligung nicht möglich ist.

Zulässigkeit der Bildbearbeitung nach biometrischen Merkmalen

Die Biometrie-Bearbeitung der Bilder wird durch die Viisage-Software vorgenommen, die als proprietäre Anwendung auf dem DIBIKO-PC installiert ist. Die Software „schneidet“ die Bilder nach den ICAO-Vorgaben so zu, dass sie für die Ausweise verwendet werden können. Die ICAO-Norm wiederum ist Grundlage der gesetzlichen Anforderungen der Anlage 3 zu § 3 PassMustV.

A4 Authentizität der Nutzer

Die „Anwender“ der DIBIKO-Fotokabine auf Seiten der Kommune werden auf zwei Ebenen authentisiert:

- Um Zugriff auf das betreffende Laufwerk zu erhalten, muss sich der Benutzer zunächst gegenüber dem zentralen Authentisierungsdienst der Kommune bzw. der Behörde authentisieren, dies kann beispielsweise ein kommunales Active Directory auf Windows-Basis sein. Diese Authentisierung erfolgt durch die Einsatzumgebung.
- Nach erfolgreicher Anmeldung auf der Ebene der Einsatzumgebung erfolgt eine Authentisierung gegenüber dem Meldewesen-Applikations-Server bzw. der Meldewesen-Anwendung: Die Authentisierung erfolgt anhand einer Benutzerkennung mit Passwort, dessen Mindestanforderungen vom Sicherheitskonzept der Behörde abhängig sind. Die Herstellerempfehlungen sehen hier eine Identität der Zugriffsberechtigungen vor.

Die genannten Authentisierungsmechanismen sorgen insgesamt dafür, dass die Authentizität der Benutzer in vollem Umfang sichergestellt wird.

A5 Authentizität des DIBIKO-PC

Die Authentizität des DIBIKO-PC (sowohl für Fotokabinen-Version als auch für SmallBusiness) wird hardwareseitig zunächst durch eine (vom Netzwerk-Administrator festgelegte) statische IP-Adresse sowie zusätzlich durch die der Netzwerkkarte fest zugeordnete MAC-Adresse sichergestellt, beide Merkmale werden beim Zugriff stets abgefragt, ein Zugriff auf die Bilddaten kann erst bei Übereinstimmung dieser Merkmale erfolgen. Des Weiteren wird in den Herstellerempfehlungen empfohlen, den DIBIKO-PC zusätzlich mit einem (Dauer-)Passwort zu versehen, mit dem er sich zusätzlich im Netzwerk identifizieren muss.

Die geschilderten Authentisierungsanforderungen sind höher als in behördlichen Netzen üblich, da dort in der Regel nur die statischen IP-Adressen, nicht aber zusätzlich auch die MAC-Adressen abgefragt werden. Sie sind als technische Sicherheitsmaßnahme daher als angemessen bis überdurchschnittlich zu bewerten.

A6 Vertraulichkeit und Integrität der Daten

Die Vertraulichkeit und Integrität der Daten wird sowohl durch die Sicherheitsmaßnahmen des Produkts, als auch im Wesentlichen durch diejenigen der das Produkt einsetzenden Behörde bestimmt.

Der Schutz vor unberechtigtem Zugriff und unberechtigter Veränderung wird zunächst durch die physikalischen Sicherungen gewährleistet: Sowohl die Armierung der Fotokabine, als auch das Panzerschloss sowie die Stahlmantelung des Ethernetkabels sorgen für Schutz vor gewaltsamem Zugriff auf die Daten. Die Small Business Version, deren Client mangels Fotokabine nicht über derartige Sicherungen verfügt, gewährleistet die Sicherheit durch die Installation im (abschließbaren) Büro des Sachbearbeiters. Die Herstellerempfehlung schreibt dies konkret vor: Die Small Business Edition darf nicht in öffentlich zugänglichen Räumen der Behörde installiert werden (s.o. Ziff. 3.2.) Für beide Installationsarten sieht die Herstellerempfehlung darüber hinaus vor, dass der DIBIKO-Rechner über keine Internet-Anbindung verfügen darf und keine weitere Dritt-Software (außer Betriebssystem-Updates) installiert werden darf.

Ergänzt werden diese Sicherheitsmaßnahmen um diejenigen der jeweiligen Behörde: Da das DIBIKO-System stets in die kommunale Netz-Infrastruktur integriert wird, unterliegt es damit den datenschutzrechtlichen Vorgaben des betreffenden Landesdatenschutzgesetzes zu technisch-organisatorischen Sicherheitsmaßnahmen (in Schleswig-Holstein § 5 Abs. 1 LDSG S-H), insbesondere dem Erfordernis dezidierter Rechtevergaben auf Betriebssystem- und Anwendungsebene. Die Herstellerempfehlungen sehen hierbei eine Kongruenz zwischen Zugriffsrechten für die eingesetzte Meldesoftware und dem DIBIKO-PC als Datenquelle vor. Wie diese in der einsetzenden Behörde praktisch umgesetzt werden, liegt in der Verantwortlichkeit der Administratoren.

Die physischen Sicherheitsmaßnahmen gewährleisten in Verbindung mit den sinnvollen Hersteller-Empfehlungen zur Einrichtung von Zugriffskontrollen angemessene Maßnahmen zum Schutz der Bilddaten vor unberechtigtem Zugriff und unberechtigter Veränderung.

A7 Verfügbarkeit der Daten

Ebenso wie zur Sicherung der Vertraulichkeit der Daten sehen die Herstellerempfehlungen auch zur Sicherung der Verfügbarkeit Hinweise vor, wie diese für die Bilddaten zu gewährleisten ist. Der DIBIKO-PC ist danach in das netzweite Backup-Konzept der Behörde einzubeziehen, welches - durch den Einsatz von proprietären Backup-Anwendungen - die Verfügbarkeit der Daten sicherstellt. Hiernach sind zeitgesteuerte Vollsicherungen sowie inkrementelle Sicherungen des Datenbestandes durchzuführen. Mit diesen Maßnahmen ist eine angemessene Sicherung der Bilddaten gegen Verlust oder Zerstörung gewährleistet.

A8 Revisionsfähigkeit

Um sicherzustellen, dass nachvollzogen werden kann, wer auf Bilddaten zugegriffen hat, sieht die Herstellerempfehlung vor, dass die Nutzung der Meldesoftware zwingend benutzerbezogen zu protokollieren ist. Da der Zugriff auf die Bilddaten stets mittelbar über die Meldesoftware erfolgt, kann mit Umsetzung dieser - ohnehin nach dem einschlägigen Landesdatenschutzgesetz erforderlichen - Sicherheitsmaßnahme auch die Protokollierung der Zugriffe auf die Bilddaten sichergestellt werden.

A9 Umsetzung der Betroffenenrechte

Grundsätzlich werden sämtliche Bilder nach Verwendung in der Meldesoftware automatisch auf dem DIBIKO-PC gelöscht. Für den Fall, dass der Betroffene sich entschließt, das Foto nicht für die Erstellung eines Passes zu verwenden, hat er mit seiner Zufallszahl die Möglichkeit, das Bild durch einen Sachbearbeiter der Behörde löschen zu lassen. Hierauf wird im Datenschutz-/Datensicherheitskonzept explizit hingewiesen. Ohne jegliches Zutun wird das Foto entsprechend der Einwilligungserklärung nach Ablauf von 3 Monaten automatisch gelöscht – auch diese Verpflichtung findet sich im Datenschutzkonzept.

Die Betroffenenrechte können mit diesen Rahmenbedingungen, insbesondere der fest eingestellten Löschfrist, überdurchschnittlich gut umgesetzt werden.

6.2 Datenschutzfördernde Merkmale

Das Produkt DIBIKO enthält folgende datenschutzfördernde Funktionen:

--- Pseudonymisierung und Datensparsamkeit

Die Bilddaten werden ausschließlich mit einer Zufallszahl als identifizierendem Merkmal gespeichert, hiermit wird der Grundsatz der Datensparsamkeit konsequent umgesetzt und zudem verhindert, dass ein Personenbezug hergestellt werden kann.

--- Vollständige Integration in die behördliche Netzinfrastruktur

Aufgrund der Tatsache, dass personenbezogene Bilddaten nicht über (im Zweifel unsichere) öffentliche Netze transportiert werden, sondern bereits mit der Datenerhebung unmittelbar im Verantwortungsbereich der speichernden Stelle gespeichert werden, wird ein hoher Schutz vor unberechtigtem Zugriff auf die personenbezogenen Daten erreicht.

--- Vorbildliche Gewährleistung der Betroffenenrechte

Die Nutzer werden vor Beginn des Datenverarbeitungsprozesses über die Verarbeitung ihrer Bilddaten informiert und können auf der Grundlage dieser Information tatsächlich über die Verwendung und Löschung ihrer personenbezogenen Daten bestimmen.

6.3 Gesamtbewertung

Aus den Bewertungen des Datenart-Anforderungsprofils ergibt sich folgende Gesamtbewertung:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart : Bilddaten (Primärdaten)		
A1	Produktbeschreibung	verständlich und aussagekräftig, in vollem Umfang sichergestellt
A2	Datensparsamkeit, Pseudonyme	in vollem Umfang sichergestellt
A3	Zulässigkeit der Datenverarbeitung	Zulässig
A4	Authentizität der Behörden-Nutzer	in vollem Umfang sichergestellt
A5	Authentizität des DIBIKO-PC	in vollem Umfang sichergestellt
A6	Vertraulichkeit und Integrität der Daten	in vollem Umfang sichergestellt
A7	Verfügbarkeit der Daten	in vollem Umfang sichergestellt
A8	Revisionsfähigkeit	in vollem Umfang sichergestellt
A9	Betroffenenrechte	in vollem Umfang sichergestellt

Oliver Stutz

Anlage 1: Protokollreport Münzen (Beispiel)

: IDS-Statusreport			
Takingreport Nr.: 0 at: 01.11.2005 (last one at: 01.11.2005)			
Vendorname: APK			
PO-Box :			
Adress: AutoPhotoKiosk			
Telephone: 0228-3509013			
Automat:			
Coins:		Pictures:	
5 coins	β € 00.50 =	2.50 €	B & W, layout1:
13 coins	β € 01.00 =	13.00 €	B & W, layout2:
181 coins	β € 02.00 =	362.00 €	B & W, layout3:
12 coins	β € 06.00 =	72.00 €	Color, layout1:
19 coins	β € 00.00 =	0.00 €	Color, layout2:
9 coins	β € 00.00 =	0.00 €	Color, layout3:
			pieces
			pieces
			pieces
			44 pieces
			pieces
			pieces
Total:	amount net:	387.50 €	Total:
	VAT:	62.00 €	
	total:	449.50 €	all layouts:
			44 pieces

Anlage 2: Protokollreport der dBase-Datenbank (Beispiel)

```

00000976|APK|20051107|10:00:06|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000977|APK|20051107|10:02:38|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000978|APK|20051107|16:44:46|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000979|APK|20051107|16:47:28|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000980|APK|20051108|19:20:58|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000981|APK|20051108|19:34:00|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
00000982|APK|20051109|09:09:45|200511|||6|600|0|||16|110|€|0050|0100|0200|0000|0000|0000|0|0|0|3|0|0|0|GER|
$$
00000976|000018f|1|
00000976|0000190|1|
00000976|0000191|1|
00000976|1|
00000977|0000192|0|
00000977|0000193|0|
00000977|0000194|1|
00000977|1|
00000978|0000195|1|
00000978|0000196|1|
00000978|0000197|1|
00000978|1|
00000979|0000198|1|
00000979|0000199|0|
00000979|000019a|1|
00000979|1|
00000980|000019b|1|
00000980|000019c|1|
00000980|000019d|0|
00000980|1|
00000981|000019e|1|
00000981|000019f|0|
00000981|00001a0|0|
00000981|1|

```

Legende:

Die Daten sind durch das Zeichen | voneinander getrennt.

Zuerst kommen Daten mit folgenden Werten

Fortlaufende Nr. (hier stets APK | Datum YYYYMMDD| Uhrzeit HH:MM:SS |Datum YYYYMM||| zu zahlender Betrag in Euro 6|gezahlter Betrag in Cent 600|Druckerstatus o|||MwSt hier noch 16|Konstant 110|Währung €|Münzer1 50 Cent|Münzer2 100|Münzer3 200|Münzer4 000|Münzer5 000| Münzer6 000|Drucklayout o|Gezahlt Münze1 - Münze6(o|o| 3|o|o|o|)|Sprache GER|

Beispiel

00000982||APK|20051109|09:09:45|200511||| 6| 600|0||| 16|110|€| 0050| 0100| 0200| 0000| 0000| 0000|0|0|0|3|0|0|0|GER|
danach \$\$ als Trennzeichen eines neuen Satzaufbaus

Danach Bilddaten mit folgenden Werten

Fortlaufende.Nr aus Teil1|fortlaufende Bildnr (Hex)|Flag ICAO Konform|

Beispiel: 00000976|000018f|1|

Anlage 3: Mustervertrag zu Support und Auftragsdatenverarbeitung

Aufstellungsvertrag

zwischen : Stadt xxx
Stadtverwaltung

(im folgenden Kunde genannt)

und Vending Concept
Paul-Kemp-Str. 4
53173 Bonn

(im folgenden VC genannt)

Die beiden Parteien vereinbaren, wie nachstehend näher erläutert, die Installation des Systems DIBIKO mit Fotokabine und deren Wartung.

1. Der Kunde stellt VC eine geeignete Stellfläche zum Betrieb eines Fotoautomaten mit System DIBIKO zur Verfügung. Der Aufstellort befindet sich
2. Die Kosten für Lieferung (nach vorheriger Terminabsprache) Aufstellung bzw. Umrüstung des/der Automaten übernimmt VC. Der Kunde stellt die ununterbrochene Lieferung von Strom sicher.
3. Der Betrieb, die technische Instandhaltung sowie Wartung gehen zu Lasten von VC. Eventuelle Betriebsstörungen und/oder Beschädigungen müssen vom Kunden unverzüglich an VC gemeldet werden. Der Kunde übernimmt nach vorheriger Absprache Kleinstreparaturen (z.B. Münzprüfer verstopft, sowie in Ausnahmefällen auch einen Papierwechsel). VC stellt den Kunden von Ansprüchen Dritter aus dem Betrieb des/der Automaten frei, soweit es Druck und Lieferung des physischen (ausgedruckten) Bildes betrifft.

Für die störungsfreie Übermittlung der Bilder von der Fotokabine zum verarbeitenden Softwareprogramm tragen die Vertragspartner gemeinsam Verantwortung. VC

verpflichtet sich, die aufgenommenen Bilder im vereinbarten Format in ein vereinbartes Austauschverzeichnis einzustellen.

4. VC rechnet monatlich mittels schriftlicher Abrechnung mit dem Kunden ab. Die monatliche Beteiligung der Kommune beträgt % der Nettoeinnahmen (d.h. Bruttoeinnahme abzüglich Mehrwertsteuer). Sie wird jeweils bis zum 25. des Folgemonats auf das nachfolgend aufgeführte Konto des Vermieters überwiesen.

Bank :

Kto.:

BLZ:

4. Das Vertragsverhältnis beginnt mit der Inbetriebnahme des/der VC Automaten und wird zunächst für einen Zeitraum von 36 Monaten abgeschlossen. Es wird eine Probezeit von 6 Monaten vereinbart. Während dieser Zeit kann der Vertrag mit vierwöchiger Frist gekündigt werden. Nach Ablauf dieser Frist beträgt die Kündigungsfrist 3 Monate zum Vertragsende. Ohne Kündigung verlängert sich der Vertrag automatisch um jeweils 12 Monate. Eine Kündigung hat mittels eingeschriebenen Briefes zu erfolgen.
5. Für Reklamationen wird im Bürgerbüro eine „Rückvergütungskasse“ eingerichtet, aus der eventuelle Reklamationen aufgrund technischer Störungen des Automaten direkt bezahlt werden können. Jede Auszahlung wird VC mit dem reklamierten Bild belegt. Auf der Rückseite des reklamierten Bildes ist die Adresse des Kunden und bei mehreren aufgestellten Automaten in einer Gemeinde zusätzlich der Standort des Automaten zu vermerken.
6. Auftragsdatenverarbeitung
 - (1) Mit der in diesem Vertrag vereinbarten Wartung von IT- Systemen der Fotokabine verarbeitet VC personenbeziehbare Daten, die der Verantwortlichkeit des Kunden unterliegen. VC wird gemäß § 11 BDSG im Rahmen einer Auftragsdatenverarbeitung für den Kunden tätig.
 - (2) Der Kunde ist für die Einhaltung des geltenden Landesdatenschutzrechts bzw. - soweit anwendbar - des BDSG und anderer Vorschriften über den Datenschutz verantwortlich. VC verarbeitet die Daten nur im Rahmen der Weisungen des Kunden.
7. Gegenseitige Pflichten der Vertragspartner
 - (1) Die Wartung erfolgt nur vor Ort in den Räumen des Kunden. Der Kunde ist berechtigt, die Wartungsarbeiten zu jeder Zeit zu verfolgen und diese jederzeit abubrechen.
 - (2) VC verpflichtet sich, die Wartung möglichst auf eine Weise durchzuführen, dass dabei keine personenbezogenen Daten zur Kenntnis genommen werden.

- (3) Die unbefugte Weitergabe von Daten, die im Rahmen der Wartung offenbart werden, ist unzulässig und kann Schadenersatzansprüche der betroffenen Personen begründen.
 - (4) Das Installieren von Daten und Software (z. B. Korrekturen, Ergänzungen des Betriebssystems bzw. der systemnahen Software oder Änderung bzw. Neuinstallation von Anwendungsprogrammen) durch VC erfolgt i.d.R. unter Testbedingungen. Die Übernahme in den Produktionsbestand oder das direkte Einspielen in die Produktionsumgebung geschieht nur auf ausdrückliche Anweisung des Auftraggebers.
 - (5) VC bestätigt, zur Durchführung des Vertrages nur Mitarbeiter oder Erfüllungsgehilfen einzusetzen, die eine Geheimhaltungsklausel unterschrieben haben und gemäß den gesetzlichen Bestimmungen verpflichtet und informiert sind (§§ 5 BDSG, 88 TKG). VC verpflichtet sich, die gleichen oder zumindest äquivalente Geheimnisschutzregeln zu beachten, wie sie der Kommune obliegen.
8. Bilder für Dienstausweise der Stadt werden gesondert vergütet.
9. Sämtliche Änderungen dieses Vertrages bedürfen der Schriftform. Gerichtsstand für beide Parteien ist Bonn.

Ort, Datum :

.....

Kunde

Vending Concept