Kriterienkatalog und Vorgehensweise zur Erlangung eines priventum-Zertifikats

datenschutz cert GmbH

Version 1.5

Inhaltsverzeichnis

Kriterienkatalog und Vorgehensweise zur Erlangung eines priventum-Zertifikats

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	13.07.2010		Initialversion	Dr. Sönke Maseberg
1.1	19.10.2010		editorielle Änderungen	Dr. Sönke Maseberg
1.2	25.10.2010		Präzisierung nach Rücksprache mit Prof. Dr. Kubicek	Dr. Sönke Maseberg
1.3	18.03.2011		Präzisierung nach Rücksprache mit Prof. Dr. Kubicek	Dr. Irene Karper Dr. Sönke Maseberg
1.4	17.05.2011		editorielle Änderungen und Präzisierungen	Dr. Sönke Maseberg
1.5	27.02.2012		Überarbeitung im Hinblick auf Veröffentlichung als Kritierenkatalog	IK, SM

Dokumenten-Überwachungsverfahren

<table>
<tr><td colspan="2">Titel: Kriterienkatalog und Vorgehensweise zur Erlangung eines priventum-Zertifikats (Regelspezifisches Zertifizierungsschema für priventum – Zertifikat für Datenschutz-Management)</td><td>Anlage ZS12 des Zertifizierungsschemas der datenschutz cert GmbH</td></tr>
<tr><td>Status: final</td><td rowspan="2">Dokument-/ Prozessbesitzer: Sönke Maseberg</td><td>Datum: 27.02.2012</td></tr>
<tr><td>Pfad, wo dieses Dokument zu finden ist: Cert:\Zertifizierung\Zertifizierungsschema</td><td>Version: 1.5</td></tr>
</table>

1. Anforderungen an ein Datenschutz-Management

In das Ende 2009 novellierte Bundesdatenschutzgesetz (BDSG) ist das zuvor intensiv und zum Teil kontrovers diskutierte Bundesdatenschutzauditgesetz nicht aufgenommen worden. Damit gibt es noch immer kein bundesweit einheitliches Auditierungsverfahren für Datenschutz, obwohl – insbesondere nach den vielen Datenschutzskandalen – ein solches Audit dringend notwendig erscheint und für viele Unternehmen und öffentliche Stellen von Interesse ist. Denn ein Datenschutzaudit – freiwillig, von Experten durchgeführt und von einer unabhängigen Zertifizierungsstelle bescheinigt – stärkt das Vertrauen von Kunden bzw. Bürgern in die geprüfte und zertifizierte Institution.

Die datenschutz cert GmbH bietet die Auditierung und Zertifizierung eines Datenschutz-Managements an. Ziel dieses „Zertifikats für vorbildlichen Datenschutz“ ist es, Unternehmen und Behörden die Möglichkeit zu geben, das Thema Datenschutz pro-aktiv und positiv zu besetzen, und dies durch ein Zertifikat nach außen hin zu dokumentieren.

Zertifiziert wird eine Institution (Scope) dahingehend, ob ein vorbildlicher Datenschutz etabliert und umgesetzt wird und ob die einschlägigen datenschutzrechtlichen Anforderungen erfüllt sind. Der Scope ist dabei einschränkbar auf einen klar abgegrenzten Bereich signifikanter Größe und mit hinreichender datenschutzrechtlicher Relevanz. Die Grundidee zur Realisierung eines vorbildlichen Datenschutzes ist dabei, Datenschutz in der Institution nachhaltig zu etablieren und die Umsetzung kontinuierlich aufrechtzuerhalten – kurz gesagt, ein Datenschutz-Management zu betreiben.

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO 27006 akkreditierte Zertifizierungsstelle und darf danach international gültige Zertifikate für ISO 27001-konforme Informationssicherheits-Managementsysteme (ISMS) erteilen.

Um die Aussagekraft eines priventum-Zertifikates sicherstellen zu können, müssen die Anforderungen an ein Datenschutz-Management öffentlich gemacht sein. Aus diesem Grund finden Sie im vorliegenden Dokument unser Zertifizierungsschema mit dem Kriterienkatalog, in dem unsere Anforderungen an ein Datenschutz-Management sowie die Datenschutzprofile normiert sind. Damit können Sie sich jederzeit überzeugen, wofür ein ausgestelltes Zertifikat steht und welche Anforderungen an die zertifizierte Institution gestellt werden. Sofern Sie Interesse daran haben, auf Grundlage unseres Zertifizierungsschemas ein Datenschutz-Management zu auditieren oder zu zertifizieren, sprechen Sie uns bitte vorher an! **Eine Nutzung unseres Zertifizierungsschemas für das Datenschutz-Management ist ohne vorherige schriftliche Zustimmung untersagt!**

Bremen, den 27. Februar 2012

Dr. Sönke Maseberg/ datenschutz cert GmbH

2. priventum-Zertifikat für Datenschutz-Management

2.1 Ausrichtung eines „Zertifikats für vorbildlichen Datenschutz“

Ziel dieses „Zertifikats für vorbildlichen Datenschutz“ ist es, Unternehmen und Behörden die Möglichkeit zu geben, das Thema Datenschutz pro-aktiv und positiv zu besetzen, und dies durch ein Zertifikat nach außen hin zu dokumentieren.

Zertifiziert wird eine Institution (Scope) dahingehend, ob ein vorbildlicher Datenschutz etabliert und umgesetzt wird und ob die einschlägigen datenschutzrechtlichen Anforderungen erfüllt sind. Der Scope ist dabei einschränkbar auf einen klar abgegrenzten Bereich signifikanter Größe und mit hinreichender datenschutzrechtlicher Relevanz.

Die Grundidee zur Realisierung eines vorbildlichen Datenschutzes ist dabei, Datenschutz in der Institution nachhaltig zu etablieren und die Umsetzung kontinuierlich aufrechtzuerhalten – kurz gesagt, ein Datenschutz-Management zu betreiben.

2.2 Datenschutz-Management

Das Datenschutz-Management sorgt für die Etablierung und nachhaltige Umsetzung der datenschutz-rechtlichen Anforderungen in einer Institution. Es umfasst alle Regelungen, die für die Steuerung und Lenkung (Planung, Umsetzung, Überwachung, Verbesserung) für die Zielerreichung der Institution zur Realisierung eines vorbildlichen Datenschutzes sorgen.

Grob orientiert sich ein solches Management an der für Managementsysteme üblichen Vorgehensweise in Form eines PDCA (Plan-Do-Check-Act)-Zyklus, vgl. etwa dazu die internationale Norm ISO 27001 oder ISO 9000, wodurch ein Datenschutz-Management in bestehende Prozesse integriert werden kann. Es enthält zudem eine strukturierte Herangehensweise, um zunächst alle relevanten Anforderungen zusammenzustellen und diese dann anschließend umzusetzen.

2.2.1 Plan-Phase

Etablieren Datenschutz-Management/Prozesse

Etablierung eines betrieblichen Datenschutzbeauftragten (bDSB) und entsprechender Managementstrukturen, damit ein vorbildlicher Datenschutz realisiert werden kann. Datenschutz ist als integraler Bestandteil der zu zertifizierenden Institution zu verstehen. Konkrete Anforderungen:

- Bestellung eines betrieblichen/behördlichen Datenschutzbeauftragten, soweit erforderlich;
- nachhaltige Fachkunde und Zuverlässigkeit des Datenschutzbeauftragten;
- Unabhängigkeit des Datenschutzbeauftragten;
- Zusammenwirken mit allen Beteiligten (Unternehmensführung, Mitarbeiter, unternehmensinterne Organe wie z.B. Betriebsrat, QM-Beauftragter, IT-Sicherheitsbeauftragter und Aufsichtsbehörden);

--- Einbindung des Datenschutzbeauftragten in relevante Prozesse (z.B. Einführung neuer Software, Entwurf von Richtlinien, Betriebsvereinbarungen, Verträgen, Auswertungen von Mitarbeiterdaten).

Istaufnahme

Strukturanalyse:

--- Identifikation und Darstellung des Untersuchungsgegenstands/ Scope:

  --- Welche Bereiche gehören dazu?

  --- Was ist datenschutz-rechtlich von Belang für die Institution?

--- Erfasst werden die folgenden Zielobjekte[1]:

  --- Organisation mit Rollen/Funktionen und Mitarbeitern;

  --- alle relevanten Gebäude;

  --- alle relevanten IT-Systeme (Server, Arbeitsplätze/Clients, Netzkomponenten, Verbindungen) mit Netzplan;

  --- alle relevanten Verfahren inkl. relevanter Datenarten.

Gesetzliche Rahmenbedingungen:

--- In diesem Abschnitt stellt der Antragsteller zunächst dar, welche Gesetze und Verordnungen für die zu zertifizierende Institution einschlägig sind. Ergänzt wird diese Zusammenstellung um datenschutzrechtliche Interpretationen.

  Bsp. §11 BDSG.

  Bsp. Datenschutzrechtliche Interpretationen (Anonymität, Pseudonymität.)

Bedrohungen:

--- Neben den gesetzlichen Rahmenbedingungen stellt der Antragsteller in diesem Abschnitt dar, welche Bedrohungen für die zu zertifizierende Institution relevant sind und welche Bedeutung der Datenschutz für die Institution darstellt.

--- Sinnvoll ist, sich auf die wesentlichen Bedrohungen zu konzentrieren und auf diejenigen Bedrohungen zu verzichten, die implizit durch die gesetzlichen Rahmenbedingungen berücksichtigt sind. Es ist nicht notwendig, die gesetzlichen Anforderungen in Bedrohungen umzuformulieren.

  Bsp. Vertrauensverlust/Imageschaden.

Abgeleitete Anforderungen/Datenschutzanforderungen:

--- Aus den direkt einschlägigen Gesetzen und Verordnungen werden in diesem Abschnitt Anforderungen abgeleitet und den Zielobjekten – soweit sinnvoll – zugeordnet, so dass sich die Möglichkeit bietet, Einzelaspekte zu

[1] Zielobjekte sind analog zum Wording bei IT-Grundschutz Einzel-Objekte des Untersuchungsgegenstands.

gruppieren, Redundanzen aufzulösen oder spezielle Aspekte zu verdeutlichen.

--- Die relevanten Datenarten werden klassifiziert.

--- In diesem Abschnitt tauchen die typischen Begriffe auf:

  --- Zutrittskontrolle;

  --- Zugangskontrolle;

  --- Zugriffskontrolle;

  --- Weitergabekontrolle;

  --- Eingabekontrolle/Revisionsfähigkeit;

  --- Auftragskontrolle;

  --- Verfügbarkeitskontrolle;

  --- Zweckbindung/Trennungsgebot;

  --- bDSB;

  --- Zulässigkeitsprüfung;

  --- Arbeitnehmerdatenschutz;

  --- Anonymität;

  --- Pseudonymität;

  --- Unbeobachtbarkeit;

  --- Nicht-Verkettbarkeit/Un-Zurechenbarkeit;

  --- Kontingenz[2];

  --- Transparenz;

  --- Datenvermeidung;

  --- Datensparsamkeit;

  --- Erforderlichkeit;

  --- Direkterhebung beim Betroffenen;

  --- Authentizität;

  --- Integrität.

--- Es wird eine Zuordnung aus den einschlägigen gesetzlichen Rahmenbedingungen und relevanten Bedrohungen auf diese abgeleiteten Anforderungen zur Sicherstellung der Vollständigkeit der Ableitung erwartet, die auch die Zielobjekte umfassen.

[2] Personenbezogene Daten werden auch dann weiterverarbeitet, wenn sie nicht widerspruchsfrei zu anderen Daten sind

Bsp. einer Tabelle, die die Zuordnung aufzeigt:

datenschutzrechtliche Rahmenbedingungen und relevante Bedrohungen	*zugeordnete abgeleitete Anforderung*	*zugeordnete Zielobjekte*	*Bemerkung zur Umsetzung*
§ 6 BremDSG	*bDSB*	*alle Mitarbeiter*	*Verpflichtung auf das Datengeheimnis der Mitarbeiter obliegt dem bDSB; vgl. dezidierte Anforderungen in BremDSG*
datenschutzrechtl. Interpretation	*Pseudonymität*	*alle Verfahren*	*für alle Verfahren ist zu prüfen, ob und wieweit eine pseudonyme Nutzung möglich ist*
Imageschaden	*Zugriffsschutz*	*alle Verfahren*	*für alle Verfahren ist ein Zugriffsschutz sicherzustellen*

Anforderungskatalog/Datenschutzziele:

--- In diesem Abschnitt stellt der Antragsteller den konkreten Anforderungskatalog zusammen, der sich aus den zuvor abgeleiteten Anforderungen ergibt.

--- Damit orientiert sich die Vorgehensweise an anderen Kriterienwerken zur Prüfung und Bewertung von Sicherheitseigenschaften, bei denen typischerweise vor der eigentlichen Überprüfung ein Anforderungskatalog zusammengestellt wird, der den eigentlichen Prüfungsmaßstab definiert.

--- Zur Aufstellung eines Anforderungskatalogs können sogenannte Datenschutzprofile im Sinne von Anforderungsprofilen verwendet werden. Diese stellen quasi einen Baukasten von Anforderungen zu verschiedenen Themenkomplexen dar, aus dem – abhängig vom konkreten Untersuchungsgegenstand – relevante Aspekte zum Anforderungskatalog herangezogen werden können, die damit den für den jeweiligen Untersuchungsgegenstand anwendbaren Prüfmaßstab darstellen.

--- Um möglichst effizient und effektiv diesen Anforderungskatalog aufstellen und um eine weitestgehende Vollständigkeit relevanter Einzelanforderungen sicherstellen zu können, wird – soweit möglich – auf anerkannte Kriterienwerke Bezug genommen; in diesem Kontext auf die internationalen

Normen ISO 27001 und ISO 27002, die einen umfangreichen Erfahrungsschatz an wichtigen Aspekten zur Informationssicherheit enthalten.[3]

--- Da spezielle Datenschutzanforderungen in diesen existierenden Kriterienwerken nicht immer in der Tiefe vorhanden sind, werden ergänzende Datenschutzprofile entwickelt.

--- Die folgenden Datenschutzprofile sind verfügbar:

  --- Datenschutz-Management;

  --- Mitarbeiter-Sensibilisierung;

  --- Physikalische Sicherheit;

  --- IT-Infrastruktur;

  --- Verfahren;

  --- Penetrationstest.

--- Dieses Modell stellt eine strukturierte Herangehensweise dar, um die relevanten Einzelanforderungen für die relevanten Zielobjekte zusammenzustellen, deren Umsetzung für die Erfüllung der zuvor abgeleiteten Anforderungen wichtig ist.

--- Hinweis: Die Auflistung der Datenschutzprofile ist nicht vollständig, d.h. es kann – auch in der Zukunft – konkrete rechtliche Anforderungen geben, für die die vorliegenden Datenschutzprofile unzureichend sind. Es ist eine Fortschreibung der Datenschutzprofile geplant.

--- *Bsp. einer Tabelle, die die Zuordnung aufzeigt:*

Datenschutzprofil	*zugeordnete, abgeleitete Anforderung*	*zugeordnete Zielobjekte*	*Bemerkung*
Datenschutz-Management	*(Standard-Datenschutz-profil)*	*(allgemein)*	*Profil ist standardmäßig anzuwenden*
Verfahren	*Zugriffskontrolle*	*alle Verfahren*	
	Eingabekontrolle	*alle Verfahren*	

[3] Alternativ ist auch eine Nutzung der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) möglich.

2.2.2 Do-Phase

Umsetzung

Umsetzung der Anforderungen lt. Anforderungskatalog; dazu kann sich der Antragsteller auch andere Zertifikate bedienen, was sich durch den Bezug der Datenschutzprofile zu existierenden Kriterienwerken anbietet.

Dokumentation

Dokumentation, wie die relevanten Aspekte des Anforderungskatalogs erfüllt werden:

- Verfahrensverzeichnis;
- Datenschutzkonzept;
- Sicherheitskonzept;
- Erfüllung des Anforderungskatalogs: Zu allen Aspekten des Anforderungskatalogs muss eine Erläuterung verfügbar sein.

Bsp. Bearbeitung des Datenschutzprofils „Verfahren" durch Beantwortung der dort thematisierten Aspekte.

Bsp. Bearbeitung des Datenschutzprofils „IT-Infrastruktur" durch Beantwortung der dort thematisierten Aspekte.

2.2.3 Check-Phase

Der bDSB checkt die Umsetzung durch lfd. Kontrollen und interne Audits:

- Detektion von Vorfällen im laufenden Betrieb;
- Überprüfung der Einhaltung der Vorgaben;
- Überprüfung der Eignung und Wirksamkeit der Maßnahmen.

Damit erfüllt der bDSB insbesondere: Überwachung der Ordnungsmäßigkeit der Datenverarbeitung gemäß § 4g Abs. Nr. 1 BDSG einschließlich der technisch-organisatorischen Sicherheitsmaßnahmen gemäß § 9 BDSG.

2.2.4 Act-Phase

Falls beim Check Defizite auffallen, werden diese im Rahmen des Prozesses zum Datenschutz-Management behoben und die Dokumentation aktualisiert.

2.3 Vorteile eines Datenschutz-Managements

Durch den ganzheitlichen Ansatz und die Prozessorientierung erhalten Sie einen guten Überblick über den Datenschutz in Ihrem Verantwortungsbereich. Sie können damit auch das „Maß" der Umsetzung der datenschutz-rechtlichen Anforderungen messen und steuern – was auch Ihr Haftungsrisiko verringern kann.

Allein durch das Etablieren eines Datenschutz-Managements werden die internen Prozesse und Verfahren besser und effizienter. Da ein etabliertes Datenschutz-Management kaum Mehraufwand bedeutet, können hier Effizienzgewinne erzielt

werden. Steigern lässt sich dies erfahrungsgemäß durch eine unabhängige Begutachtung und Zertifizierung.

Da sich Märkte und Anforderungen bewegen und immer häufiger den Nachweis zu bestimmten Standards fordern, sind Sie mit einem überprüften Datenschutz-Management bestens gerüstet, auch in Zukunft neue Anforderungen schnell zu erfüllen und die Einhaltung nachzuweisen.

3. Kriterienkatalog/ Datenschutzprofile

In diesem Abschnitt sind die verfügbaren Datenschutzprofile aufgeführt. Datenschutzprofile sind im Sinne eines Anforderungsprofils aufzufassen.

3.1 Datenschutzprofil „Datenschutzmanagement“

3.1.1 Kurzbeschreibung

Das Datenschutzprofil „Datenschutzmanagement“ thematisiert Anforderungen zu übergreifenden organisatorischen Aspekten des Datenschutzes.

„Datenschutzmanagement“ wird analog zum IT-Grundschutz-Baustein „Datenschutz“ wie folgt definiert:

> Mit Datenschutzmanagement werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Der Prozessansatz eines Datenschutzmanagements ist wie bei internationalen Normen ISO 9001 oder ISO 27001 in Form eines PDCA-Zyklus’ definiert, in dem die Phasen Plan, Do, Check und Act einen Kreislauf bilden.

3.1.2 Anforderungen

Aus dem Prozessansatz in Form eines PDCA-Zyklus’ ergeben sich lt. ISO 27001 die folgenden relevanten, und z.T. auf Datenschutzbelange adaptierten Anforderungen:

PDCA-Zyklus

PLAN-Phase [27001, Abs. 4.2.1][4]:

- Definition des Geltungsbereiches, vgl. [27001, Abs. 4.2.1 a)];
- Strukturanalyse mit Liste der Assets, vgl. [27001, Abs. 4.2.1 d)];
- Auswahl der Maßnahmen mit Hilfe der Datenschutzprofile [27001, Abs. 4.2.1 e)-g)].

DO-Phase [27001, Abs. 4.2.2]:

- Umsetzung der in der PLAN-Phase identifizierten Maßnahmen, etwa zur Schulung (vgl. [27001, Abs. 5.2.2]).

CHECK-Phase [27001, Abs. 4.2.3]:

- regelmäßige Audits (vgl. [27001, Abs. 6]).

ACT-Phase [27001, Abs. 4.2.4]:

- Umsetzung von Korrekturmaßnahmen inkl. Aktualisierung, Dokumentation (vgl. [27001, Abs. 8]).

[4] ISO/IEC 27001:2005, „Information technology – Security techniques – Information security management systems requirements specification".

Dokumentationsanforderungen [27001, Abs. 4.3]

Datenschutzkonzept und Verfahrensverzeichnis sowie Sicherheitskonzept, in dem insb. die Aspekte der PLAN-Phase aus [27001, Abs. 4.2.1] dokumentiert sind [27001, Abs. 4.3.1].

Verfahrensverzeichnis erfüllt die Anforderungen des § 4g Abs. 2 Satz 1 BDSG i.V.m. § 4e BDSG:

- Zusammengefasst enthält ein Verfahrensverzeichnis zunächst für alle Verfahren gemäß § 4e Ziff. 1-3 BDSG:
  - Name und Anschrift der verantwortlichen Stelle sowie
  - Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen.
- Zu jedem Verfahren werden folgende Angaben erfasst:
  - Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung gemäß § 4e Ziff. 4 BDSG;
  - Kurzbeschreibung – sofern zur Erläuterung des Verfahrens sinnvoll –;
  - betroffene Personengruppe gemäß § 4e Ziff. 5 BDSG;
  - Datenkatalog oder Datenkategorien gemäß § 4e Ziff. 5 BDSG;
  - Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können, gemäß § 4e Ziff. 6 BDSG;
  - Regelfristen für die Löschung der Daten gemäß § 4e Ziff. 7 BDSG;
  - geplante Datenübermittlung in Drittstaaten gemäß § 4e Ziff. 8 BDSG;
- Separat werden zudem zu jedem Verfahren folgende Angaben angegeben:
  - Zugriffsberechtigte gemäß § 4g Abs. 2 BDSG;
  - technisch-organisatorische Maßnahmen nach § 4e Ziff. 9 BDSG i.V.m. § 9 BDSG.

  Die Angaben können ggf. als Referenz auf Datenschutz- oder Sicherheitskonzept vorliegen.

Aufzeichnungen aus internen Audits [27001, Abs. 4.3.1];

eindeutige Kennzeichnung der Dokumente, Aktualität, Freigabe [27001, Abs. 4.3.2].

Verantwortung des Managements [27001, Abs. 5]

Bestellung eines betrieblichen/behördlichen Datenschutzbeauftragten, soweit erforderlich:

- nachhaltige Fachkunde, Zuverlässigkeit, Unabhängigkeit des Datenschutzbeauftragten;

--- Zusammenwirken mit allen Beteiligten (Unternehmensführung, Mitarbeiter, unternehmensinterne Organe wie z.B. Betriebsrat, QM-Beauftragte, IT-Sicherheitsbeauftragter und Aufsichtsbehörden);

--- Einbindung des Datenschutzbeauftragten in relevante Prozesse (z.B. Einführung neuer Software, Entwurf von Richtlinien, Betriebsvereinbarungen, Verträgen, Auswertungen von Mitarbeiterdaten).

Schulungen, Bewusstsein und Kompetenz [27001, Abs. 5.2].

Interne Audits [27001, Abs. 6]

Durchführung interner Audits, geplant und gegen die Anforderungen mit Stichproben.

Management-Bewertung [27001, Abs. 7]

Feedback an Management.

Verbesserung [27001, Abs. 8]

stetige Verbesserung.

Weitere Anforderungen:

Konzeption der DO-, CHECK- und ACT-Phasen

Leitlinie mit Fokus Datenschutz, vgl. [27002, A.5][5]:

--- Leitlinie veröffentlichen, genehmigen, verteilen, vgl. [27002, A.5.1.1];

--- Leitlinie regelmäßig überprüfen, vgl. [27002, A.5.1.2];

Interne Organisation, vgl. [27002, A.6]:

--- Genehmigungsverfahren, vgl. [27002, A.6.1.4];

--- Vertraulichkeitsvereinbarungen, vgl. [27002, A.6.1.5];

--- Kontakt zur Community, vgl. [27002, A.6.1.7];

--- Umgang mit Externen, vgl. [27002, A.6.2.1];

Konzept zur Aktualisierung des Verfahrensverzeichnisses;

Ggf. Veröffentlichung des Verfahrensverzeichnisses für jedermann;

Durchführung von Vorabkontrollen;

Eingaben oder Beschwerden zum Datenschutz/Betroffenenrechte;

Konzept zur Auswahl und Überwachung der Auftragnehmer, die gemäß § 11 BDSG Datenverarbeitung im Auftrag durchführen;

[5] ISO/IEC 27002, „Information technology – Security techniques – Code of practice for information security management".

Konzept zur Überwachung der Ordnungsmäßigkeit der Datenverarbeitung gemäß § 4g Abs. Nr. 1 BDSG einschließlich der technisch-organisatorischen Sicherheitsmaßnahmen gemäß § 9 BDSG.

Melden von Vorfällen, vgl. [27002, A.13]

Melden von Vorfällen, vgl. [27002, A.13.1];

Umgang mit Vorfällen, vgl. [27002, A.13.2];

Compliance, vgl. [27002, A.15]

Identifikation anwendbarer Gesetze, vgl. [27002, A.15.1.1];

Datenschutz und Vertraulichkeit personenbezogener Informationen, vgl. [27002, A.15.1.4].

3.2 Datenschutzprofil „Mitarbeiter-Sensibilisierung“

3.2.1 Kurzbeschreibung

Das Datenschutzprofil „Mitarbeiter-Sensibilisierung“ thematisiert mit der Sensibilisierung von Mitarbeitern eine zentrale Anforderung des Datenschutzes. Das Datenschutzprofil umfasst auch Telearbeiter und sonstige Mitarbeiter, die von unterwegs aus auf personenbezogene Daten zugreifen und diese verarbeiten. Sofern zulässig, sind besondere Anforderungen an die Sicherheit umzusetzen.

3.2.2 Anforderungen

Aspekte dieses Datenschutzprofils zur Sensibilisierung von Mitarbeitern:

- Verpflichtung von Mitarbeitern auf das Datengeheimnis nach § 5 BDSG, vgl. auch [27002, Abs. A.8.1.3];
- Schulung und Sensibilisierung, vgl. [27002, Abs. A.8.2.2];
- Zugänglichkeit datenschutzrelevanter Informationen;
- tatsächlicher Motivations- und Sensibilisierungsgrad der Mitarbeiter und der Unternehmensführung auf das Thema Datenschutz;
- Einhaltung von Richtlinien, Betriebsvereinbarungen o.Ä. zu Vorgaben des Datenschutzes.

Sensibilisierung bei Mobile Computing/Telearbeit:

- Mobile Computing und Telearbeit, vgl. [27002, Abs. A.11.7];
  - Mobile Computing und Kommunikation, vgl. [27002, Abs. A.11.7.1];
  - Telearbeit, vgl. [27002, Abs. A.11.7.2].

3.3 Datenschutzprofil „Physikalische Sicherheit“

3.3.1 Kurzbeschreibung

Das Datenschutzprofil „Physikalische Sicherheit“ thematisiert Anforderungen zu Gebäuden und Räumen, in denen Einrichtungen und Systeme untergebracht werden, um personenbezogene Daten zu verarbeiten.

3.3.2 Anforderungen

Für alle Verfahren, in denen personenbezogene Daten verarbeitet werden, sind die folgenden Anforderungen zu prüfen und zu bewerten:

- Physische und umgebungsbezogene Sicherheit [27002, Abs. A.9]:
  - Zutrittskontrolle, vgl. [27002, Abs. A.9.1.2];
  - Sichere Entsorgung, vgl. [27002, Abs. A.9.2.6].

3.4 Datenschutzprofil „IT-Infrastruktur“

3.4.1 Kurzbeschreibung

Das Datenschutzprofil „IT-Infrastruktur“ thematisiert Anforderungen zur virtuellen Sicherheit von Systemen, mit denen personenbezogene Daten verarbeitet werden.

3.4.2 Anforderungen

Für alle Systeme, mit denen personenbezogene Daten verarbeitet werden, sind die folgenden Anforderungen zu prüfen und zu bewerten:

- Betriebs- und Kommunikationsmanagement, vgl. [27002, Abs. A.10];
  - Änderungsmanagement und Freigabe, vgl. [27002, Abs. A.10.1.2];
  - Schutz vor Schadsoftware, vgl. [27002, Abs. A.10.4];
  - Backup, vgl. [27002, Abs. A.10.5];
  - Netzmanagement, vgl. [27002, Abs. A.10.6.1];
  - Entsorgung von Medien, vgl. [27002, Abs. A.10.7.2];
  - Umgang mit Informationen, vgl. [27002, Abs. A.10.7.3];
  - Austausch von Informationen, vgl. [27002, Abs. A.10.8.1];
  - Transport von Informationen, vgl. [27002, Abs. A.10.8.3];
  - Auditprotokolle, vgl. [27002, Abs. A.10.10.1];
- Zugangskontrolle, vgl. [27002, Abs. A.11];
  - Regelwerk/ Dokumentation, vgl. [27002, Abs. A.11.1.1];
  - Benutzerregistrierung, vgl. [27002, Abs. A.11.2.1];
  - Überprüfung, vgl. [27002, Abs. A.11.2.4];
  - Passwörter, vgl. [27002, Abs. A.11.3.1];

- --- Zugangskontrolle für Netze, vgl. [27002, Abs. A.11.4.1];
- --- Zugangskontrolle auf Betriebssystemebene, vgl. [27002, Abs. A.11.5.1];
- --- Identifikation und Authentisierung, vgl. [27002, Abs. A.11.5.2];
- --- Rückgabe Zugangsrechte, vgl. [27002, Abs. A.8.3.3];

- --- Weitergabekontrolle/kryptographische Maßnahmen, vgl. [27002, Abs. A.12.3];
  - --- Verwaltung kryptographischer Schlüssel, vgl. [27002, Abs. A.12.3.2];
  - --- Eignung kryptographischer Verfahren;
- --- Authentizität/Integrität/Herkunft der Daten;
- --- Eingabekontrolle/Revisionsfähigkeit:
  - --- Protokollierungen des traffics (in/out)/der Nutzer;
  - --- Protokollierung von Datenänderungen: Was? Durch wen?
  - --- Sicherung der Protokolle gegen nachträgliche Veränderung.

3.5 Datenschutzprofil „Verfahren“

3.5.1 Kurzbeschreibung

Das Datenschutzprofil „Verfahren“ thematisiert auf Anwendungsebene Anforderungen an Verfahren, mit denen personenbezogene Daten verarbeitet werden – auch Internetseiten. Das Datenschutzprofil „Verfahren“ beschreibt auch Anforderungen zur rechtlichen Zulässigkeit einer Datenverarbeitung personenbezogener Daten sowie Anforderungen zu datenschutz-rechtlichen Prinzipien.

3.5.2 Anforderungen

Für alle Verfahren, in denen personenbezogene Daten verarbeitet werden, sind die folgenden Anforderungen zu prüfen und zu bewerten:

- --- rechtliche Zulässigkeit;
- --- speziell für Auftragsdatenverarbeitung sind Anforderungen aus § 11 BDSG einschlägig;
- --- Zugriffskontrolle, vgl. [27002, Abs. A.11]:
  - --- Zugriffskontrolle auf Applikationsebene, vgl. [27002, Abs. A.11.6];
  - --- Einschränkung der Zugriffsberechtigungen, vgl. [27002, Abs. A.11.6.1];
- --- Berechtigungs- bzw. Rollenkonzept für Anwendungen:
  - --- Entwicklungs-, Test- und Produktionssystem (2- oder dreistufiges System);
  - --- Entwicklung bzw. Test mit Echtdaten;
  - --- Administration (Rollen zur Berechtigungsvergabe, zum Anlegen neuer Benutzer, etc.);

- --- Prozess der Berechtigungsvergabe und Softwarefreigabe;
- --- Umfang der Wartung durch externe Dienstleister;
- --- Authentisierungsmechanismen (Passwort, Token, Zertifikat etc.);
- --- Login-Parameter (u.a. Mindestlänge, Höchstgültigkeitsdauer der Passwörter);
- --- Existenz einer Rollenbeschreibung;
- --- Berechtigungsmatrix (welche Anwender sind im Besitz welcher Rolle);
- --- Change Management (wer hat wann worauf zugegriffen bzw. Rechte vergeben?);
- --- Zweckbindung/ Datentrennung/ unterschiedliche Verschlüsselung?

--- Mechanismen um sicherzustellen, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

--- Prüfung „Datenschutz-rechtliche Prinzipien“:

- --- Hinweis: Sofern ein Aspekt nicht einschlägig ist, kann er mit Begründung entfallen.
- --- Transparenz der Datenverarbeitung (z.B. Datenschutzerklärung und Impressum bei Internetseiten oder Verfahrensregister);
- --- Datenvermeidung;
- --- Datensparsamkeit;
- --- Erforderlichkeit;
- --- Pseudonymität;
- --- Anonymität;
- --- Nicht-Verkettbarkeit;
- --- Kontingenz: „Personenbezogene Daten werden auch dann weiterverarbeitet, wenn sie nicht widerspruchsfrei zu anderen Daten sind“;
- --- Direkterhebung beim Betroffenen.

3.6 Datenschutzprofil „Penetrationstest“

3.6.1 Kurzbeschreibung

Das Datenschutzprofil „Penetrationstest“ thematisiert Anforderungen zu ergänzenden Tests, um die Umsetzung der Regelungen und Vorgaben zu prüfen.

3.6.2 Anforderungen

Für alle Systeme und Verfahren, in denen personenbezogene Daten verarbeitet werden, sind die folgenden Tests durchzuführen:

- --- externe Tests;

--- Ermittlung der Ports bzw. Dienste;

--- Ermittlung der Reaktionszeit zum Sperren der Tests;

--- Test der Web-Applikation.

4. Auditierungs- und Zertifizierungsprozess

In diesem Abschnitt wird vorgestellt, wie die datenschutz cert GmbH ein Datenschutz-Management auditiert und zertifiziert. Abbildung 1 illustriert den Life-Cycle eines Zertifikates zum Datenschutz-Management.

Dabei wird ein zwei-stufiges Zertifizierungsverfahren eingesetzt:

--- Der bei der datenschutz cert GmbH lizenzierte Auditor prüft die Konformität eines Datenschutz-Managements gegen die o.g. Kriterien und erstellt einen Auditreport.

--- Die Zertifizierungsstelle prüft den Auditreport, insbesondere um eine Vergleichbarkeit zwischen den Audits sicherstellen zu können.

4.1 Laufzeiten

Jedes Zertifizierungsverfahren besteht aus folgenden Phasen:

--- Erst-Zertifizierung;

--- 1. Überwachungsaudit (1 Jahr nach Erst-Zertifizierung);

--- 2. Überwachungsaudit (2 Jahre nach Erst-Zertifizierung);

--- Re-Zertifizierung (3 Jahre nach Erst-Zertifizierung).

Nachfolgend ist in Abbildung 1 der Lebenszyklus eines Zertifikates dargestellt.

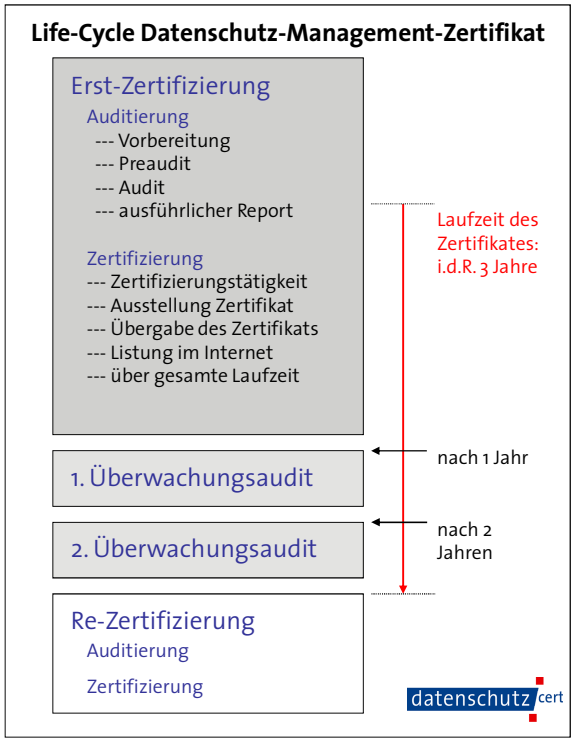

Abbildung 1: Lebenszyklus eines priventum-Zertifikates

4.2 Auditierung

Die vom der datenschutz cert GmbH lizenzierten Auditoren prüfen das Datenschutz-Management.

Grundidee ist dabei: Der Auditor prüft das Datenschutz-Management auf höherer „Meta"-Ebene; dazu wird der Auditor den Prozess des Datenschutz-Managements wie folgt begutachten und beurteilen:

- Prüfung der Plausibilität, Nachvollziehbarkeit und Vollständigkeit der Istaufnahme, insb. sind dabei folgende methodischen Schritte zu beleuchten:
  - Ableitung aus den einschlägigen Gesetzen und Verordnungen sowie Bedrohungen auf die Anforderungen samt Bezug zum Untersuchungsgegenstand;
  - Zusammenstellung des Anforderungskatalogs aus den Datenschutzprofilen;
  - Sinnhaftigkeit explizit dargelegter Datenschutzprofile;
  - Sinnhaftigkeit der Zusammenstellung von Maßnahmen und Controls aus anderen Kritierenwerken;
- Vollständigkeit der Umsetzung: D.h. enthält die Dokumentation zu allen Aspekten des Anforderungskatalogs entsprechende Hinweise zur Umsetzung.
- Stichprobe, ob die dokumentierte Umsetzung korrekt ist. Die Stichprobe muss angemessen sein und besonders sensible Bereiche hinreichend erfassen.

Analog zur Auditierung eines ISMS erfolgt die Prüfung und Bewertung in drei Phasen:

- Vorbereitung;
- Preaudit;
- Audit.

In einer Vorab-Prüfung (Preaudit) werden erste Ergebnisse auf dem Weg zu einem Zertifikat und ggf. notwendige Verbesserungen identifiziert.

Anschließend erfolgt die eigentliche Prüfung: Das Audit besteht aus Dokumentenprüfung sowie Site Visit: Für jeden relevanten Aspekt prüft und dokumentiert der Auditor, wie Sie lt. Dokumentation diesen Aspekt umsetzen und ob die in der Dokumentation angegebenen Maßnahmen umgesetzt sind. Das Datenschutzaudit umfasst alle bestehenden Prozesse des Datenschutz-Managements. Die Bewertung berücksichtigt, ob Maßnahmen getroffen werden, die über das gesetzlich geforderte Maß an Datenschutz-Management hinausgehen (diese werden als vorbildlich bewertet) oder ob „angemessene" / „adäquate" oder „gesetzeskonforme" Maßnahmen getroffen oder nicht umgesetzt werden.

Die Ergebnisse werden in einem aussagekräftigen Auditreport dokumentiert und der Zertifizierungsstelle vorgelegt.

4.3 Zertifizierung

Die Zertifizierungsstelle prüft auf Grundlage des Auditreports sowie weiterer relevanter Informationen, ob das Audit gemäß den Vorgaben durchgeführt wurde und trifft final die Entscheidung, ob das Datenschutz-Management konform zu unseren Anforderungen betrieben wird und erteilt dann ein Zertifikat.

Das nach ISO 27006 aufgestellte Zertifizierungsschema der datenschutz cert GmbH, welches eine Grundlage für die Akkreditierung als Zertifizierungsstelle darstellt, wird auch für diese Zertifizierung genutzt.

4.4 Überwachungsaudit

Nach Erteilung Ihres Zertifikats ist jährlich ein Überwachungsaudit zur Aufrechterhaltung des Zertifikats durchzuführen.

4.5 Re-Zertifizierung

Nach Ablauf des (i.d.R.) drei Jahre gültigen Zertifikats kann ein Re-Zertifizierungsaudit durchgeführt werden, dass sich im Wesentlichen an der Erst-Zertifizierung orientiert und zusätzlich die kontinuierliche Wirksamkeit Ihres Managementsystems feststellen soll.

4.6 Auditoren

Aufgrund der technischen und rechtlichen Anforderungen, muss sich der Auditor für beide Bereiche (rechtlich und technisch) lizenzieren lassen; es ist eine Begrenzung der Lizenzierung auf einen der Bereiche möglich.

Fachkunde: 5 Jahre analog zu ISO 27006

Es ist möglich, eine Prüfstelle als Auditor zu lizenzieren, sofern der Leiter der Prüfstelle eine entsprechende Fachkunde nachweist und verantwortlich zeichnet.

4.7 Logo

Für ein zertifiziertes Datenschutz-Management kann ein Kunde ein Logo verwenden, das die folgenden Inhalte/Anforderungen enthält:

- Angabe des Regelwerks: priventum;
- Logo/Name der Zertifizierungsstelle;
- ID des Zertifikats, evtl. mit Jahreskennung;
- Ablaufdatum.

Darüber hinaus erhält ein Kunde für ein zertifiziertes Datenschutz-Management ein Zertifikat, welches folgende Informationen enthält:

- den Namen des Kunden;
- eine exakte Beschreibung des Untersuchungsgegenstands/ Geltungsbereich;
- Datum zur Erteilung, Erweiterung oder Erneuerung der Zertifizierung, wobei Datum nicht vor dem Datum der Zertifizierungsentscheidung liegen darf;

--- das Ablaufdatum oder das Fälligkeitsdatum zur Re-Zertifizierung, das im Einklang mit dem Re-Zertifizierungszyklus steht;

--- Hinweis zum letzten Audittag;

--- Zertifizierungs-ID;

--- Angaben zum angewendeten Regelwerk;

--- Angaben zur Zertifizierungsstelle.

4.8 Zertifikatsliste

Eine Liste unserer erteilten Zertifizierungen kann abgerufen werden unter: http://www.datenschutz-cert.de/zertlisten/. Aus der Liste sind der Antragsteller, der Geltungsbereich, die Zertifikats-ID sowie die Gültigkeit der Zertifizierung ersichtlich.

4.9 Entzug eines Zertifikates

Das Zertifikat wird entzogen, wenn der Antragsteller nachhaltig gegen die Zertifizierungsvoraussetzungen verstößt. Ein solcher Verstoß liegt insbesondere vor, wenn

--- der zertifizierte Untersuchungsgegenstand in der beschriebenen Weise verändert wurde und der Anbieter keine Prüfung ermöglicht

--- im Rahmen der Prüfung nicht die für die Vergabe des Zertifikats erforderlichen Voraussetzungen erfüllt werden,

--- der Antragsteller aufgrund drohender oder eingetretener Insolvenz einen zuverlässigen Geschäftsbetrieb nicht mehr aufrechterhalten kann

--- die Zertifizierungskosten nicht spätestens innerhalb von 4 Wochen nach Abschluss der Zertifizierung gegenüber der Zertifizierungsstelle beglichen werden.

Die Zertifizierungsstelle teilt dem Antragsteller die Gründe des Zertifikatsentzugs mit. Im Falle des Entzuges wird das über die Zertifikatsliste online unter www.datenschutz-cert.de veröffentlichte Zertifikat auf den Status als entzogen gesetzt und spätestens nach 4 Wochen aus der Liste entfernt. Der Entzug des Zertifikates kann auch anderweitig veröffentlicht werden.

4.10 Ablauf eines Zertifikates

Soweit das Zertifikat nach Ablauf der Gültigkeit entfällt, hat der Anbieter dafür zu sorgen, dass das Logo und sämtliche Hinweise auf eine gültige Zertifizierung aus den genutzten Medien unverzüglich entfernt werden.

4.11 Kosten und Gebühren

Kosten fallen einerseits für die Auditierung, andererseits für die Zertifizierung an.

Das Honorar für die Durchführung des Audits und des Überwachungsaudits ist i.d.R. abhängig von der Komplexität des Auditgegenstands und wird zwischen dem Auditor und dem Antragsteller individuell vereinbart und abgerechnet. Die datenschutz cert GmbH kann ein Gesamtangebot für eine Auditierung und Zertifizierung abgeben, sofern ein eingesetzter Auditor bei ihr angestellt ist.

Die für die Zertifizierung anfallenden Kosten begleichen den gesamten Zertifizierungsvorgang (Prüfung des Audit-Reports, Korrespondenz, Zertifikatsverwaltung sowie – bei Zertifikatsvergabe - die Nutzungsrechte). Die Kosten fallen an, sobald ein Antrag auf Zertifizierung oder der Audit-Report bei der Zertifizierungsstelle eingegangen ist. Erteilt die Zertifizierungsstelle einen Ablehnungsbescheid, werden die Kosten anteilig berechnet.

Die Höhe der Zertifizierungskosten richtet sich nach der Komplexität des Prüfaufwands. Dieser bestimmt sich u.a. nach den Funktionen des Untersuchungsgegenstands, dem Umfang der Datenverarbeitung, der Umgebung für das Datenschutzmanagement, den vorgelegten Informationen und dem Umfang der Korrespondenz aller Beteiligten. Auf Wunsch kann die Zertifizierungsstelle – *vor Antragstellung* – eine kostenlose Einschätzung der Zertifizierungskosten erstellen.

4.12 AGB

Im Übrigen sind die Allgemeinen Geschäftsbedingungen der datenschutz cert GmbH zu beachten, die unter www.datenschutz-cert.de abgerufen werden können.

5. Anforderungen an einen Auditreport

Ein Auditreport zur Vorlage bei der Zertifizierungsstelle muss inhaltlich mindestens zu folgenden Aspekten Stellung beziehen:

- Organisatorische und formale Angaben zum Audit:
  - das mit der Auditierung angestrebte Zertifikat;
  - Untersuchte Organisation, Name, Anschrift, Standort;
  - genaue Bezeichnung des Untersuchungsgegenstands, Abgrenzung zu den nicht auditierten Bereichen;
  - Auditoren (Recht/Technik), Name, Anschrift;
  - Zeitraum der Auditierung;
- Angewandte Methodik: z.B. Prüfung von Dokumenten des Auftraggebers, Führung von Mitarbeitergesprächen, Durchführung von Stichproben vor Ort (Site Visit) oder Plausibilitätstests;
- Grundlagen der Auditierung:
  - eingesehene Dokumente;
  - befragte Abteilungen/Arbeitsbereiche/Unternehmensorgane;
  - Gegenstand der Stichproben;
  - Ortsbesichtigung, Standort, Adresse, Dauer, Teilnehmer;
- Erklärung der Auditoren zur Unabhängigkeit und Unparteilichkeit;
- Kurzdarstellung des Untersuchungsgegenstands;
- Zusammenstellung des für den konkreten Auditgegenstand anwendbaren Prüfkriterien/Anforderungen;
- Auditergebnisse:
  - Prüfung und Bewertung aller Prüfpunkte des Kriterienkatalogs;
- Votum des Auditors mit:
  - Zusammenfassung der Auditergebnisse / Management Summary;
  - Vorschlag an die Zertifizierungsstelle.

6. datenschutz cert GmbH

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der datenschutz nord-Gruppe. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg.

6.1 Leitlinien

Die datenschutz cert GmbH bietet Konformitätsbewertungen unter folgenden grundsätzlichen Leitlinien an:

6.1.1 Unabhängigkeit und Unparteilichkeit

Wir sind unabhängig und unparteilich. Es gilt das übergeordnete Interesse und die vorrangige Pflicht, Auditierungen, Evaluierungen, Zertifizierungen und Bestätigungen entsprechend den Vorgaben frei von internen und externen kommerziellen, finanziellen und sonstigen Zwängen durchzuführen. Maßstab ist das jeweilige Kriterienwerk. Zudem führen wir keinerlei Beratung durch.

Wir haben einen "Ausschuss zur Sicherstellung der Unparteilichkeit der datenschutz cert GmbH" (Ausschuss) etabliert, mit dem die grundsätzlichen Regelungen zur Unabhängigkeit und Unparteilichkeit der Zertifizierungstätigkeiten diskutiert und durchgeführte Zertifizierungsprozesse auf ihre Unabhängigkeit hin überprüft werden.

Zur Gewährleistung der Unabhängigkeit und Unparteilichkeit unserer erteilten Zertifikate setzen wir für den Auditierungs- und Zertifizierungsprozess darüber hinaus regelmäßig externe Fachbegutachter ein.

6.1.2 Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

6.1.3 Offenheit und Transparenz

Wir sind offen und transparent hinsichtlich unser Tätigkeiten, d.h.

- wir kommunizieren klar und unmissverständlich, was und nach welchen Regeln geprüft und zertifizieren wird;
- unsere Zertifikate und Auditreports sind klar und verständlich formuliert;
- wir veröffentlichen die zugrundeliegenden Regelwerke - sofern nicht durch Copyright geschützt -;
- wir benennen klar, wofür wir akkreditiert sind;
- wir lassen uns selber regelmäßig auditieren;
- wir sind offen für alle Anfragen und Beschwerden: Wenn Sie Fragen zu einem von uns erteilten Zertifikat haben oder potentiell den Missbrauch eines Zertifikats vermuten: Bitte sprechen Sie uns an. Wir sichern Ihnen Ver-

traulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

6.1.4 Datenschutz

Wir kommen aus dem Datenschutz. Jede Art von Konformitätsprüfung wird - im Rahmen des jeweiligen Untersuchungsgegenstands - unter den besonderen Aspekten des Datenschutzes beleuchtet. Dadurch stellen wir sicher, dass die von uns geprüften und bewerteten IT-Produkte und -Systeme den Anforderungen des Datenschutzes genügen.

Unser Anspruch ist, dass sich "datenschutz certifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

6.2 Akkreditierungen

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO 27006 akkreditierte Zertifizierungsstelle für ISO 27001-konforme Informationssicherheits-Managementsysteme und setzt das Zertifizierungsschema auch für das Zertifikat zum Datenschutz-Management ein.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditiert und ist danach berechtigt, Evaluierungen gemäß Common Criteria (CC) durchzuführen.

Die datenschutz cert GmbH ist darüber hinaus als Gutachter des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein akkreditiert. Die Akkreditierung gilt sowohl für den Bereich Technik als auch für den Bereich Recht.

Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle gemäß Signaturgesetz.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-/ ISO 27001-Auditoren.

6.3 Kontakt

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0421.69 66 32-50
Fax: 0421.69 66 32-51
E-Mail: office@datenschutz-cert.de
Internet: www.datenschutz-cert.de