Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Hauptabteilung Staats- und Verwaltungsrecht
Abteilung Rechtsetzungsprojekte und -methodik

Verordnung über die Datenschutzzertifizierungen: Erläuterungen

Der Entwurf stützt sich auf Artikel 11 Absatz 2 der Änderung des Bundesgesetzes über den Datenschutz vom 24. März 2006 (in der Folge: revDSG)[1], der vorsieht, dass der Bundesrat Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens erlässt. Der Entwurf nimmt den bereits in der Botschaft umschriebenen Rahmen für die Datenschutzzertifizierungen auf (vgl. Botschaft Revision DSG, BBl 2003 2136 f.). Er sieht zwei Zertifizierungsobjekte – Organisation und Verfahren des Datenschutzes (Datenschutzmanagementsystem) sowie Produkte (Hardware, Software oder Systeme für automatisierte Datenbearbeitungsverfahren) – vor. Als Grundanforderung an die Zertifizierungsstellen ist vorgesehen, dass diese über eine Akkreditierung verfügen müssen. Damit besteht Gewähr für eine einheitliche Kontrolle der Zertifizierer, zudem kann der Regelungsbedarf stark reduziert werden. Die Verordnung legt im Übrigen einige Minimalanforderungen betreffend die Zertifizierungsstellen sowie das Zertifizierungsverfahren fest.

Im Hinblick auf die Einführung eines Datenschutz-Qualitätszeichens wurden zwei Varianten geprüft:

- Verzicht auf ein offizielles Qualitätszeichen: Es bliebe ausschliesslich den Privaten (insb. Zertifizierungsstellen) überlassen, selbst Qualitätszeichen festzulegen und den Zertifizierten – i.d.R. gegen Bezahlung einer Lizenzgebühr – das Verwendung des Zeichens gestatten. In dieser Variante werden in der Verordnung nur die Anforderungen an die Zertifizierung geregelt, die für alle Qualitätszeichen zu erfüllen wären.
- Festlegung eines offiziellen Qualitätszeichens: Nach dieser Variante würde in der Verordnung ein offizielles Qualitätszeichen vorgesehen, das von den zertifizierten Stellen ohne weitere Bedingungen verwendet werden kann. Das bedeutet indessen nicht, dass Zertifizierungen von einer staatlichen Stelle durchgeführt würden. Dieses offizielle Qualitätszeichen wäre eine Art „Infrastrukturdienstleistung“ und würde zusätzlich zu allfälligen privaten Qualitätszeichen bestehen.

In beiden Fällen wäre als organisatorisches Modell zudem eine gemischte Trägerschaft denkbar. Diese Lösung wurde jedoch aus Ressourcengründen ausgeschlossen.

Für die Variante „Verzicht auf ein offizielles Zeichen“ spricht in erster Linie ein grundsätzliches Argument: Mit der Einführung der Datenschutzzertifizierungen soll die Rechtsdurchsetzung im Datenschutzbereich auf privater Basis verbessert werden. Die Kontrolltätigkeit wird teilweise "privatisiert", was mit einem privaten DSQ adäquat

---

1 Referendumsvorlage BBl 2006 3547

zum Ausdruck gebracht würde. Als weiteren Vorteil dieser Variante lässt sich anführen, dass die Privatinitiative bezüglich der DSQ gewahrt wird. Zudem kann die Regelungsdichte der Verordnung gesenkt werden. Als möglicher Nachteil erscheint, dass eine unübersehbare Vielfalt an Datenschutz-Qualitätszeichen entstehen und damit die Markttransparenz beeinträchtigt werden könnte. Schwierigkeiten könnten zudem entstehen, wenn Inhaber von Qualitätszeichen die gesetzlichen Vorgaben nicht (oder nicht mehr) einhalten.

Mit dem offiziellen Qualitätszeichen könnte einer Label-Flut indirekt entgegengewirkt werden. Es würde zudem sicherstellen, dass alle zertifizierten Stellen auch Zugang zu einem solchen Zeichen haben, was in der ersten Variante nicht absolut gewährleistet ist. Ein weiterer Vorteil würde darin liegen, dass die Zertifizierung kostengünstiger ist, da weder die Zertifizierer noch die Zertifizierten für das Qualitätszeichen Lizenzgebühren bezahlen müssen. Die Variante bringt zwei wesentliche Nachteile: Zum Einen würde ein staatlicher Eingriff in einen bisher den Privaten überlassenen Markt erfolgen, zum Andern müsste die Regelungsdichte der Verordnung erhöht werden.

Nach Evaluation der mit den beiden Varianten verbundenen Vor- und Nachteile wird die erstgenannte Variante bevorzugt. Ihre Vorteile sind klar greifbar und werden insbesondere auch deshalb höher gewichtet als die Nachteile, weil bei diesen ungewiss ist, ob sie sich überhaupt realisieren werden.

1. Anforderungen an die Zertifizierungsstellen (Art. 1)

Die Voraussetzungen, welche die Zertifizierungsstellen zu erfüllen haben, ergeben sich grundsätzlich aus den ISO/IEC Guides 62 (neu ISO/IEC 17021) und 65 (wird demnächst ebenfalls ISO-Norm), deren Anwendbarkeit in Art. 7 Abs. 1 und Anhang 2 der Akkreditierungs- und Bezeichnungsverordnung (AkkBV; SR 946.512) geregelt ist. Dort wird namentlich das Unabhängigkeitserfordernis festgelegt und das Zertifizierungs- bzw. Produkteprüfungsverfahren geregelt. Eine zusätzliche Regelung in dieser Verordnung erübrigt sich.

Zu konkretisieren sind dagegen die Anforderungen an die Qualifikation der Auditorinnen und Auditoren bzw. des Personals, welches Produkteprüfungen durchführt. Es ist dabei zu berücksichtigen, dass es im Bereich des Datenschutzes keine standardisierten Ausbildungen gibt und dass Expertinnen und Experten vergleichsweise rar sind. Entsprechende Praxiserfahrung ist daher zu berücksichtigen. Die entsprechenden Anforderungen werden im Anhang konkretisiert.

Absatz 3 verwendet in Anlehnung an die Bio-Verordnung (SR 910.18) den Begriff des Kontrollprogramms. Dieses Kontrollprogramm umfasst einerseits den Prüfungsraster, der inhaltlich vorgibt, welche Standards in welchen Punkten zu erfüllen sind sowie Angaben zum Ablauf des Kontrollverfahrens (einschliesslich der Überwachung und der Reevaluation). Zu zertifizierende "Stellen" im Sinne von Buchstabe a dieser Bestimmung können sowohl Bundesorgane als auch private Organisationen sein. Auch eine Arztpraxis oder Anwaltskanzlei, wo regelmässig Daten bearbeitet werden, ist eine „Stelle“ im Sinne dieser Bestimmung und kann damit sich damit zertifizieren lassen.

Die Mindestanforderungen (Abs. 4) richten sich in erster Linie nach den internationalen Standards, deren Anwendbarkeit sich aus der Akkreditierungs- und Bezeich-

nungsverordnung ergibt. Durch den Verweis auf die Art. 4 bis 6 der vorliegenden Verordnung wird verdeutlicht, dass auch die einschlägigen datenschutzrechtlichen Regelungen Teil der Mindestanforderungen sind.

2. Beizug des EDÖB im Akkreditierungsverfahren (Art. 2)

Diese Bestimmung stellt eine Konkretisierung von Art. 11 Abs. 1 und 2 AkkBV dar.

3. Anerkennung ausländischer Zertifizierungsstellen (Art. 3)

Da im Bereich des Datenschutzes (noch) kein international harmonisierter Akkreditierungsstandard besteht und kein entsprechendes Verfahren definiert ist, muss die Anerkennung ausländischer Zertifizierungsstellen hier geregelt werden. Die Bestimmung entspricht Art. 29 Bio-Verordnung.

4. Zertifizierung von Datenschutzmanagementsystemen (Art. 4)

4.1 Allgemeines

Absatz 1 macht die Unterscheidung zwischen verschiedenen Auditierungs- bzw. Zertifizierungsobjekten deutlich.

Absatz 2 hält in genereller Art und Weise fest, was im Rahmen des Audit-Verfahrens zu begutachten ist. Die Kriterien umschreiben den Inhalt eines so genannten Datenschutzmanagementsystems: Es ist dies zunächst die Datenschutzpolitik. Die Datenschutzpolitik ist ein Grundlagendokument, welches die Grundzüge des Datenschutzes in der betreffenden Organisation vorgibt und die entsprechende Selbstverpflichtung aufzeigt; sie beschreibt den Ansatz der organisatorischen Massnahmen, mittels derer die Vorschriften des Datenschutzgesetzes sowie weitere gegebenenfalls zu beachtende Datenschutzbestimmungen eingehalten werden sollen. Daraus leitet sich die Konzeption der Umsetzung der datenschutzrechtlichen Vorschriften sowie ggf. internationaler Standards, die eine "gute Praxis" im Bereich Datenschutz und Datensicherheit umschreiben, in ihren Einzelheiten ab. Weiter sind Gegenstand des Audit-Verfahrens die Massnahmen, die vom betreffenden Datenbearbeiter zur Verwirklichung der festgehaltenen Datenschutzziele und -Massnahmen getroffen wurden. Besonderes Gewicht liegt dabei auf der Einrichtung von Verfahren zur Behebung festgestellter Probleme und Mängel.

Absatz 3 hält fest, dass der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem erlässt (vgl. Ziff. 4.2 unten).

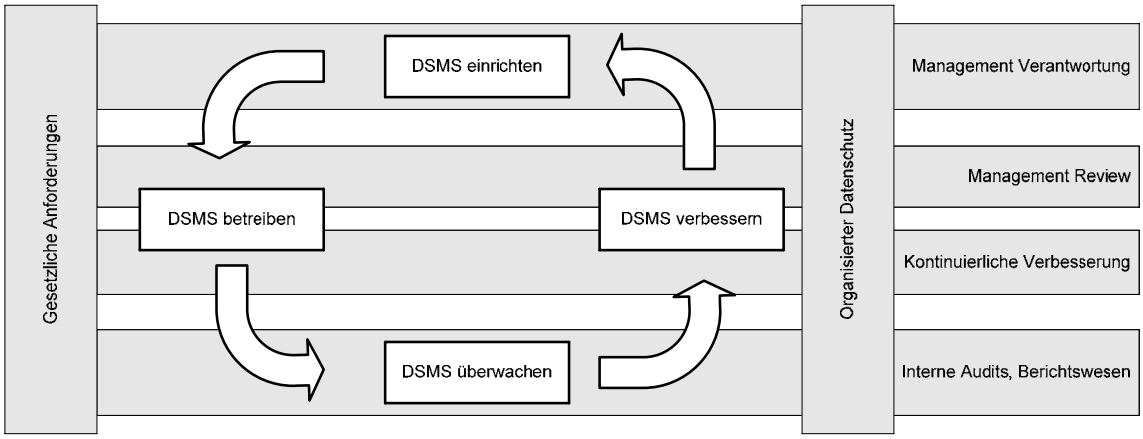
Absatz 4 präzisiert die Formulierung vom Art. 11a Abs. 5 revDSG. Er macht deutlich, dass nur dann von der Anmeldung einer Datensammlung abgesehen kann, wenn sämtliche Datenbearbeitungen, die im Rahmen der Zweckbestimmung dieser Datensammlung anhand der darin enthaltenen Daten vorgenommen werden, Gegenstand einer Zertifizierung waren.

4.2 Mindestanforderungen an das Datenschutzmanagementsystem

4.2.1 Das Datenschutzmanagementsystem als Managementsystem

Absatz 3 verweist auf die Mindestanforderungen, die ein Datenschutzmanagementsystem erfüllen muss. Insbesondere wird der ISO-Standard 27001:2005 für Informationssicherheit erwähnt[2]. Damit wird nicht nur deutlich, dass ein Zusammenhang zwischen Datenschutz und Informationssicherheit besteht, sondern auch, dass das Datenschutzmanagementsystem nach den gleichen Grundsätzen funktioniert, wie bestehende standardisierte Managementsysteme in anderen Bereichen. Es kann daher auch ohne weiteres in bestehende Managementsysteme (z.B. ein Qualitätsmanagementsystem) eingegliedert werden.

Das Datenschutzmanagementsystem basiert, wie auch verwandte Managmentsysteme, auf dem sog. PDCA-Modell (Plan-Do-Check-Act = festlegen-durchführen-prüfen-handeln oder einrichten-betreiben-überwachen-verbessern). Es hat eine stetige Verbesserung des Datenschutzes in der betreffenden Organisation zum Ziel.



Der Aufbau und die Umsetzung eines Datenschutzmanagementsystems (DSMS) bestimmen sich nach den gesetzlichen Anforderungen und werden namentlich beeinflusst durch Zweck und Umfang der vorgenommenen Bearbeitungen von Personendaten, den dabei eingesetzten Mitteln sowie die Grösse und die Struktur der Organisation.

Das organisationsbezogene DSMS folgt einem Prozessansatz, der seiner Entwicklung, Umsetzung, Durchführung, Überwachung, Aufrechterhaltung und kontinuierlichen Verbesserung dient. Das sog. PDCA-Modell (Plan-Do-Check-Act; festlegen-durchführen-prüfen-handeln oder einrichten-betreiben-überwachen-verbessern) ist auf alle DSMS-Prozesse anzuwenden.

Das DSMS ist ein Managementsystem, das mit anderen Managementsystemen verträglich geführt werden kann. Die Darstellung des DSMS ist freigestellt. Anderweitige Managementsysteme bzw. Zertifikate z.B. ISO 27001:2005 können massgebliche Elemente an das DSMS beitragen. Allerdings berechtigen solche Zertifikate nicht, ohne spezifische Nachprüfung die Zertifizierungsaussage auf das DSMS zu übertragen.

---

[2] SN ISO/IEC 27001:2005 (kann bei der Schweizerischen Normenvereinigung bezogen werden)

4.2.2 Inhaltliche Umschreibung

Die Einrichtung des DSMS erfolgt gestützt auf die Definition von Anwendungsbereich, Datenschutzpolitik (vgl. Ziff. 4.1) und der Methode zur Risikoeinschätzung betreffend Datensicherheit. Die sich aus den Datenschutzgrundsätzen (vgl. Art. 4 ff. DSG) und weiteren rechtlichen Grundlagen ergebenen Anforderungen sind zu identifizieren und Datensicherheitsrisiken sind einzuschätzen. Darauf gestützt sind entsprechende Massnahmen zu bestimmen und durch das Management zu genehmigen.

Im Rahmen der Umsetzung der festgelegten Massnahmen sind Verfahren vorzusehen, die eine sofortige Erkennung von und Reaktion auf Unregelmässigkeiten ermöglichen und geeignet sind, Datenschutzverletzungen zu identifizieren und zu beheben.

Die Wirksamkeit des DSMS ist regelmässig zu überprüfen, namentlich mittels interner Audits in mindestens jährlichen Abständen. Dabei identifizierte Verbesserungsmöglichkeiten (Korrektur- und Vorbeugungsmassnahmen) sind umzusetzen.

Zum DSMS ist eine Dokumentation zu erstellen. Sie muss namentlich eine Erklärung zur Datenschutzpolitik enthalten, den Anwendungsbereich des DSMS umschrieben sowie die Methodik zur Risikoeinschätzung betreffend die Datensicherheit (und deren Ergebnis) beschreiben. Weiter muss sie einen Plan zur Einhaltung der Anforderungen des Datenschutzes und einen Plan zum Umgang mit den Risiken für die Datensicherheit beinhalten. Verfahren, die die Organisation zur Sicherstellung der wirksamen Planung, Durchführung und Kontrolle der Datenschutzpolitik dienen, sind ebenfalls zu dokumentieren. Die Dokumente sind vor ihrer Herausgabe von der zuständigen Stelle zu genehmigen. Sie sind laufend zu überprüfen und im Bedarfsfall zu aktualisieren. Änderungen und aktueller Status der Dokumente sind zu kennzeichnen. Die zuständigen Stellen und Personen müssen über die aktuellen Fassungen der für sie jeweils einschlägigen Dokumente verfügen.

Als Nachweis dafür, dass das DSMS wirksam ist und den Anforderungen entspricht sind entsprechende Aufzeichnungen (Logfiles etc.) zu erstellen und zu verwalten.

Das Management muss eine Reihe von Verantwortlichkeiten wahrnehmen. Darunter fällt zunächst namentlich die Entwicklung der Datenschutzpolitik, die Bestimmung von Rollen und Verantwortlichkeiten für den Datenschutz, die Bestimmung des für die Datensicherheit akzeptablen Risikoniveaus und die Durchführung von Verbesserungen. Das Management muss zudem für die Bereitstellung der Ressourcen sorgen, die erforderlich sind, um einen adäquaten Datenschutz durch richtige Anwendung aller implementierten Massnahmen aufrecht zu erhalten und die Wirksamkeit des DSMS soweit notwendig zu verbessern. Das Management sorgt weiter für eine angemessene Bewusstseinsförderung beim betreffenden Personal sowie für dessen kompetente Schulung im Bereich des Datenschutzes. Das Management muss in mindestens jährlichen Abständen – u.a. gestützt auf die Ergebnisse der internen DSMS-Audits, Ergebnisse von Wirksamkeitsmessungen und organisationsinterne und –externe Änderungen, die sich auf das DSMS auswirken können – das DSMS überprüfen und bewerten, um dessen Angemessenheit und Wirksamkeit sicherzustellen bzw. zu verbessern. Ziele dieser Managementbewertung sind insbesondere die Aktualisierung der Risikoeinschätzung und des Risikobehandlungsplans für die Datensicherheit, die bedarfsgerechte Änderung der Verfahren zur Gewährleistung des Datenschutzes (soweit interne oder externe Ereignisse dies erfordern), die Er-

kennung von Ressourcenbedürfnissen sowie die Verbesserung der Kriterien zur Messung der Wirksamkeit der Massnahmen.

5. Zertifizierung von Produkten (Art. 5)

5.1 Allgemeines

Absatz 1 umschreibt, welche Produkte Gegenstand der Zertifizierung darstellen können sollen. Eine Datenschutzzertifizierung scheint nicht nur sinnvoll für Produkte, deren eigentlicher Zweck die Datenbearbeitung ist. Ebenso sinnvoll ist die Zertifizierung von Produkten, bei deren Benutzung Personendaten anfallen. Zu denken ist dabei insbesondere an Internetbrowser, Software für den Betrieb von Webservern, Applikationen zur Betreibung von Websites, aber z.B. auch an Logistiksysteme, die auf RFID- oder GPS-Technologien beruhen.

Absatz 2 Buchstabe a verweist auf die technischen Massnahmen, wie sie sich namentlich aus Art. 8 VDSG ergeben. Ein diesbezüglicher internationaler Standard besteht mit den Common Criteria (CC 2.1/ISO 15408) und den daraus für bestimmte Kategorien von Produkten abgeleiteten Schutzprofilen, die bestimmte Sicherheitsanforderungen definieren. Ausschlaggebend dafür, welche konkreten Anforderungen sich aus dieser Bestimmung ableiten, ist der jeweils aktuelle Stand der Technik.

Buchstabe b umschreibt den Grundsatz der Datensparsamkeit bzw. Datenvermeidung, der eine Konkretisierung des datenschutzrechtlichen Verhältnismässigkeitsgrundsatzes darstellt (Art. 4 Abs. 2 DSG).

Buchstabe c verweist auf die Transparenz der Bearbeitungsvorgänge, die das Produkt gewährleisten soll. Der Nutzer soll erkennen können, welche Personendaten wie bearbeitet werden und insbesondere, welche Daten wohin übermittelt werden. Die Anforderungen werden sich dabei nach dem Benutzerkreis richten, für den das Produkt konzipiert ist; sie werden damit für ein Produkt, das für die breite Masse der Anwenderinnen und Anwender bestimmt ist höher sein, als für ein Produkt, welches nur von Spezialisten bedient wird. Zu beurteilen sind Bearbeitungen, die ein Produkt im Rahmen der Funktionalität, für die es konzipiert wurde, automatisiert vornimmt. Ist das Produkt offen ausgestaltet und kann es für unterschiedliche Zwecke verwendet oder unterschiedlich konfiguriert werden, so wird darauf zu achten sein, dass sich Mechanismen, welche die Transparenz gewährleisten sollen, durch den Datenbearbeiter nicht ohne Weiteres umgehen oder ausschalten lassen.

Buchstabe d verweist auf die technischen Massnahmen zur Unterstützung des Anwenders bei der Einhaltung weiterer, in den Buchstaben a–c noch nicht angesprochener Datenschutzgrundsätze und -pflichten. Zu denken ist beispielsweise an eine durch das zu zertifizierende Produkt unterstützte Wahrung des Zweckbindungsgebots, die automatisierte Kontrolle bzw. Beschränkung der Verknüpfung von Elementen einer Datenbank, die systemgestützte Kontrolle der Bekanntgabe von Personendaten an Dritte, die Unterstützung des Anwenders bei der Erfüllung der Auskunftspflichtsowie Funktionen zur Umsetzung von Löschungs- und Berichtigungsansprüchen.

5.2 Mindestanforderungen an die Produkteprüfung

Absatz 3 hält fest, dass der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) Richtlinien darüber erlässt, welche datenschutzzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts mindestens zu prüfen sind. Im Gegensatz zur Situation bei der Zertifizierung von Datenschutzmanagementsystemen bestehen hier keine international anerkannten Standards, die ohne Weiteres angepasst werden können.

Die Bestimmung lässt dem EDÖB eine gewisse Frist für den Erlass der Richtlinien für die Zertifizierung. Gegenwärtig laufen auf europäischer Ebene Bestrebungen zur Erarbeitung von standardisierten Vorgaben für die Datenschutzzertifizierung von Produkten. Es dürfte angezeigt sein, vor dem Erlass eigener Richtlinien zunächst den Verlauf dieser Arbeiten zu beobachten.

Denkbar ist auch, dass sich der EDÖB bei den Vorgaben für ein Begutachtungsraster für Produkteprüfungen an den Anforderungskatalog anlehnt, wie er vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein für Produkteprüfungen ausgearbeitet wurde[3]. Dieser Anforderungskatalog stellt beispielhaft Datenschutz- und Datensicherheitsanforderungen sowie in ihrem Zusammenhang zu berücksichtigende Fragestellungen nach wichtigen Rechtsnormen dar. Er gibt eine Mustergliederung für das Abarbeiten von Anforderungen. Eine reine Prüfcheckliste fällt dagegen nicht in Betracht, da sich die Anforderungsprofile und Datenarten pro zu prüfendem IT-Produkt unterscheiden und ausserdem die Prüfer ihre Bewertungen stets begründen müssen.

Die Richtlinien sollen Anforderungen an die Technikgestaltung formulieren. Dies betrifft insbesondere die Datenvermeidung und die Transparenz der Datenbearbeitung.

Die Zulässigkeit der angestrebten Datenverarbeitung wird anhand einer Konkretisierung der einschlägigen Datenschutzgrundsätze (Art. 4 ff. DSG) zu überprüfen sein.

Ebenfalls zu untersuchen wird sein, welche technisch-organisatorischen Massnahmen zum Schutz der Betroffenen das Produkt unterstützt. Diese Massnahmen leiten sich in erster Linie aus den Art. 8 ff. VDSG ab. Beachtet werden muss bei der Bewertung, welches Angreifermodell den getroffenen bzw. zu treffenden Massnahmen zugrunde liegt, gegen welche Angriffe Schutzmassnahmen vom IT-Produkt selbst vorgesehen sind, welche zusätzlichen Massnahmen unterstützt werden (bzw. ob es dabei Einschränkungen gibt), und schliesslich, welche Restrisiken verbleiben.

Weiter wird die Umsetzung der Rechte der Betroffenen (z.B. Benachrichtigung, Auskunft, Transparenzgebote) beurteilt werden müssen. Die Gewährleistung der Betroffenenrechte wird heutzutage vielfach auf organisatorischer Ebene abgedeckt. Beim zu zertifizierenden IT-Produkt ist entscheidend, inwieweit dort technisch:

- die Wahrnehmung der Rechte direkt durch die Betroffenen ermöglicht oder sogar gefördert sowie
- die organisatorische Ebene beim Betreiber zur Gewährleistung der Betroffenenrechte unterstützt wird.

---

[3] Anforderungskatalog V1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH (http://www.datenschutzzentrum.de/download/anford.pdf).

Es sind jeweils zusätzlich sowohl die Aspekte der Datensparsamkeit (z.B. ist eine Abwicklung anonym oder unter Pseudonym möglich) als auch der Protokollierung der Wahrnehmung der Betroffenenrechte zu berücksichtigen.

Schliesslich ist zu beachten, dass innerhalb eines Produktes verschiedene Datenarten verarbeitet und zwischen einzelnen Komponenten ausgetauscht werden. Beispielhaft seien hier *Betroffenendaten* (häufig auch als Primärdaten bezeichnet), z.B. Patientendaten einer Versicherung, und *Sekundärdaten* (z.B. Protokolldaten über Dateneingaben und Datenbankzugriffe, aber auch über Konfigurationsänderungen oder Zugang zu sensiblen Räumen wie Rechenzentrum) genannt.

6. Erteilung und Gültigkeit der Zertifizierung (Art. 6)

Absatz 1 macht deutlich, dass die Anforderungen, die eine zu zertifizierende Organisation oder ein zu zertifizierendes Produkt zu erfüllen haben, sich einerseits aus den einschlägigen datenschutzrechtlichen Bestimmungen und andererseits aus den in den entsprechenden Richtlinien des EDÖB zum Ausdruck gebrachten Anforderungen ergeben. Künftig werden allenfalls europäische oder internationale Normen und Standards für die Datenschutzzertifizierung vorliegen. Sollte dies der Fall sein – und soweit die darin enthaltenen Anforderungen den Richtlinien des EDÖB gleichwertig sind – kann eine Zertifizierung auch aufgrund solcher Normen und Standards erfolgen.

Die Dauer für der Gültigkeit einer Datenschutzzertifizierung für Organisation und Verfahren (Datenschutzmanagementsystem) wird in Absatz 2 auf drei Jahre festgelegt. Weiter wird ausdrücklich festgehalten, dass jährlich eine Reevaluation der erteilten Zertifizierungen zu erfolgen hat (vgl. die entsprechende Vorschrift in ISO/IEC Guide 62, Ziff. 3.6.1). Die Zertifizierungsstelle muss ein entsprechendes Überwachungsdispositiv einrichten.

Auch bei der Produktezertifizierung besteht eine analoge Pflicht (Abs. 3): Die zertifizierten Produkte müssen spätestens alle zwei Jahre neu begutachtet werden. Wenn wesentliche Veränderungen am Produkt vorgenommen werden, die sich auf die Bearbeitung von Personendaten auswirken, muss die erneute Zertifizierung sofort erfolgen (ISO/IEC Guide 65, Ziff. 13). Handelt es sich um geringfügige Änderungen, so ist eine summarische Prüfung ausreichend.

Nach Ablauf der Gültigkeitsfrist muss wiederum das vollständige Zertifizierungsverfahren durchlaufen werden, um erneut eine Zertifizierung zu erhalten.

7. Anerkennung ausländischer Datenschutzzertifizierungen (Art. 7)

Es scheint sinnvoll, einen Mechanismus vorzusehen, um auch ausländische Zertifizierungen anzuerkennen. So könnten insb. auch solche Organisationen eine Entbindung von der Pflicht zur Anmeldung ihrer Datensammlungen erlangen, bei welchen die Datenschutzzertifizierung im Ausland durchgeführt wurde. Dies könnte etwa dann der Fall sein, wenn ein Unternehmen sich in Deutschland datenschutzzertifizieren lässt, und das Zertifizierungsverfahren auch einen Unternehmensteil einschliesst, der sich in der Schweiz befindet. Der Beauftragte hat zu beurteilen, ob die Kriterien, nach denen die Zertifizierungen durchgeführt werden, materiell den Anforderungen der schweizerischen Gesetzgebung entsprechen.

8. Mitteilung des Ergebnisses des Zertifizierungsverfahrens an den EDÖB (Art. 8)

Diese Bestimmung nimmt Bezug auf Art. 11a Abs. 5 Bst. f revDSG. Sie hält klar fest, welche Unterlagen dem EDÖB einzureichen sind, um die Anforderungen ordnungsgemäss zu erfüllen. Welche Informationen der Bewertungsbericht und die Zertifizierungsdokumente umfassen müssen, ist in ISO/IEC Guide 62, Ziff. 3.4 und 3.5 umschrieben. Die Zertifizierungsdokumente enthalten Angaben über die Zertifizierungsstelle, welche die Zertifizierung durchgeführt hat, die normativen Grundlagen der Zertifizierung, die Prozesse bzw. Dienstleistungen, welche zertifiziert wurden sowie das Gültigkeits- und das Ablaufdatum der Zertifizierung. Der Bewertungsbericht enthält darüber hinaus detaillierte Angaben zur Konformität des DSMS mit den Zertifizierungsanforderungen und muss insb. Nichtkonformitäten klar nennen. Er kann ausserdem Vergleiche mit den Ergebnissen früherer Audits enthalten. Er muss schliesslich allfällige Differenzen zwischen Zertifizierungsstelle und zertifizierter Stelle zum Ausdruck bringen.

Im vorliegenden Zusammenhang ist darauf hinzuweisen, dass der Beauftragte im Rahmen seiner Aufsichtstätigkeit nach Art. 27 und 29 DSG selbstverständlich auch auf weitere mit der Zertifizierung zusammenhängende Dokumente zugreifen kann, soweit dies im Rahmen seiner Abklärungen erforderlich ist.

Aus dem Verweis auf Art. 4 folgt auch, dass nur bei einer Zertifizierung des Datenschutzmanagementsystems eine Befreiung von der Pflicht zur Registrierung der Datensammlungen möglich ist. Die blosse Verwendung zertifizierter Produkte durch einen Datenbearbeiter bzw. Inhaber der Datensammlung kann dafür nicht ausreichen, denn sie bietet nicht hinreichende Gewähr für die Einhaltung der Datenschutzvorschriften. Mit der vorliegenden Bestimmung wird klargestellt, wie Art. 11a Abs. 5 Bst. f revDSG im Zusammenhang mit Art. 11 Abs. 1 revDSG zu verstehen ist.

9. Sistierung und Entzug der Datenschutzzertifizierung (Art. 9)

Werden bei der regelmässigen Überprüfung der Zertifizierung oder bei der Rezertifizierung schwerwiegende Mängel festgestellt, kann die Zertifizierungsstelle die Datenschutzzertifizierung sistieren oder entziehen. Ein schwerer Mangel liegt insbesondere vor, wenn wesentliche Voraussetzungen der Datenschutzzertifizierung nicht mehr erfüllt sind. Dies wäre z.B. dann der Fall, wenn wiederholt festgestellt wird, dass die Dokumentationsanforderungen (vgl. Ziff. 4.2.2) nicht erfüllt werden oder dass die Managementbewertung (vgl. Ziff. 4.2.2) wiederholt nicht vorgenommen wird. Ebenfalls ein schwerer Mangel liegt vor, wenn die Zertifizierung missbräuchlich verwendet wird. Dies wäre etwa dann der Fall, wenn die Zertifizierung nur einen Teil der Datenbearbeitungen umfasst (Art. 4 Abs. 1 Bst. b) und dennoch ein Qualitätszeichen verwendet wird, welches eine umfassende Zertifizierung zum Ausdruck bringt.

Die Sanktionsmöglichkeit sieht schon der ISO/IEC-Guide 62 vor (künftig ISO/IEC 17021[4]; Ziff. 3.7.3, Anmerkung 6), der eine für die Akkreditierung massgebliche Grundlage darstellt. Es handelt sich also hier eigentlich um eine deklaratorische Be-

[4] Zeitpunkt des Inkrafttretens ist noch nicht bekannt.

stimmung, die indessen der Klarheit halber in der Verordnung verankert werden soll. Die Einzelheiten der Regelung von Sistierung und Entzug sind denn auch nicht in der Verordnung festzulegen. Zu beachten ist darüber hinaus namentlich, dass mit der vorliegenden Bestimmung *nicht* die Kompetenz zum Erlass einer Verfügung an die Zertifizierer delegiert wird. Absatz 2 hält ausdrücklich fest, dass sich bei Streitigkeiten sowohl das Verfahren als auch die materielle Beurteilung nach den einschlägigen vertragsrechtlichen Bestimmungen richten.

10. Verfahren bei Aufsichtsmassnahmen des EDÖB (Art. 10)

Bei der Datenschutzzertifizierung geht es in erster Linie um Rechtsbeziehungen zwischen Privaten, die grundsätzlich dem privaten Recht unterstehen. Dies entspricht dem Konzept der Selbstregulierung: Mit der Zertifizierung sollen Marktmechanismen dafür genutzt werden, das Datenschutzrecht besser durchzusetzen.

Die oder der Beauftragte soll daher nicht direkt in dieses privatrechtliche Rechtsverhältnis eingreifen. Stellt er – namentlich im Rahmen seiner Aufsichtstätigkeit – schwerwiegende Mängel fest, muss er aber eine Möglichkeit haben, wirksam auf die Einhaltung der gesetzlichen Vorschriften hinzuwirken. Art. 10 skizziert das Verfahren, das dafür zur Anwendung kommen soll. Er kann aber die Zertifizierung nicht selbst sistieren oder entziehen.

Stellt die oder der Beauftragte fest, dass wesentliche Voraussetzungen der Datenschutzzertifizierung nicht erfüllt sind oder dass die Zertifizierung in irreführender oder missbräuchlicher Art und Weise verwendet wird, so soll er sich zunächst an die zuständige Zertifizierungsstelle wenden, und diese über die festgestellten Mängeln unterrichten (Abs. 1). Es obliegt dann der Zertifizierungsstelle, auf die zertifizierte Organisation einzuwirken und zu veranlassen, dass die erforderlichen Massnahmen getroffen werden. Wird der Mangel nicht innert 30 Tagen durch die zertifizierte Stelle korrigiert, so sistiert die Zertifizierungsstelle die Zertifizierung. Besteht auch nach Ablauf dieser Frist gar keine Aussicht darauf, dass innert einem angemessenen Zeitraum ein rechtskonformer Zustand geschaffen oder wiederhergestellt wird, ist die Zertifizierung zu entziehen (Abs. 3). Als angemessen werden höchstens 3 Monate gelten können.

Wenn die Probleme nicht durch die Intervention der Zertifizierungsstelle behoben werden können und diese dennoch die Zertifizierung nicht sistiert oder entzieht, ist die oder der Beauftragte verpflichtet, eine Empfehlungen nach Art. 27 Abs. 4 oder 29 Abs. 3 DSG auszusprechen. Je nachdem, wem die Verantwortung für die Mängel zuzuordnen ist, kann sich eine Empfehlung an das zertifizierte Unternehmen oder die Zertifizierungsstelle richten. Wird die Empfehlung an die Zertifizierungsstelle gerichtet, so ist die Schweizerische Akkreditierungsstelle darüber zu informieren, denn sie hat die Fachaufsicht über die Zertifizierungsstellen inne. Wird die Empfehlung nicht befolgt oder abgelehnt, kann sie auf gerichtlichem Weg durchgesetzt werden[5]: Die oder der Beauftragte kann sie dem Bundesverwaltungsgericht zum Entscheid vorlegen, der Weiterzug ans Bundesgericht ist möglich.

---

[5] Nach geltendem Recht ist dies nur im privatrechtlichen Bereich möglich (Art. 29 Abs. 4 DSG); mit Inkrafttreten der Revision wird dies aber auch im Rahmen der Aufsicht über die Bundesorgane der Fall sein (neuer Art. 27 Abs. 6 DSG)

Liegen gravierende Mängel vor (z.B. wenn die Zertifizierungsstelle durch Täuschung dazu gebracht wird, eine Zertifizierung zu erteilen oder wenn falsche Zertifikate geführt werden), wäre zu prüfen, ob im konkreten Fall strafrechtliche Tatbestände erfüllt sind (Betrug, Täuschung etc.).

Schliesslich ist noch darauf hinzuweisen, dass betroffene Konkurrenten, Kunden und gewisse Organisationen, namentlich Konsumentenschutzorganisationen, in Fällen, in denen Zertifikate oder Qualitätszeichen geführt werden, ohne dass die entsprechenden Voraussetzungen gegeben sind, auch Klage nach Art. 9 und 10 des Bundesgesetzes gegen den unlauteren Wettbewerb (SR 241) führen könnten.

11. Mindestanforderung an die Qualifikation des Personals der Zertifizierungsstellen (Anhang)

Der Anhang umschreibt die Minimalqualifikationen, über die das Personal einer Zertifizierungsstelle verfügen muss, welche Datenschutzzertifizierungen durchführen will. Da es kaum Spezialisten gibt, welche sämtliche Anforderungen erfüllen, wird die Durchführung von Audits und Produkteprüfungen durch interdisziplinäre Teams, welche insgesamt die geforderten Qualifikationen aufweisen, ausdrücklich als zulässig erklärt.