Erläuterungen

zum Ablauf des Rezertifizierungsverfahrens

für die Vergabe von Datenschutz-Gütesiegeln

beim ULD SH

Version 1.0 Stand 12.3.2004

Erläuterungen zum Ablauf des Rezertifizierungsverfahrens

1 Einleitung

Das ULD vergibt Datenschutz-Gütesiegel für die Dauer von zwei Jahren. Diese Begrenzung der Laufzeit schafft den Ausgleich zwischen der Planungssicherheit der Antragsteller und der dynamischen Entwicklung der juristischen und technischen Rahmenbedingungen im Bereich der Informationstechnologie. Nach Ablauf von zwei Jahren ist daher in jedem Fall eine Rezertifizierung geboten – unabhängig von Änderungen des Produktes: Es muss überprüft werden, ob das Produkt den nun gültigen Anforderungen in technischer und rechtlicher Hinsicht genügt.
Aber auch innerhalb der zweijährigen Laufzeit der Gütesiegelzertifizierung gibt es Konstellationen, die eine Rezertifizierung erforderlich machen können: Der Zyklus von Produktänderungen liegt insbesondere im Software-Bereich deutlich unter zwei Jahren, so dass Antragsteller[1] noch während der Laufzeit von zwei Jahren ihr Produkt ändern, an neuere technische oder rechtliche Gegebenheiten anpassen oder durch Updates oder Patches Fehler beheben. Berühren diese Änderungen die Vorschriften über Datenschutz und Datensicherheit in erheblichen Maße, so ist schon vorher eine Rezertifizierung nötig. Das neue Gütesiegel hat dann eine Laufzeit von zwei Jahren. Das Verfahren zur Beurteilung von Produktänderungen und die ggf. notwendige Rezertifizierung sind bewusst einfach gehalten, um für die Antragsteller einen Anreiz zu schaffen, ihre Produkte auch während der Gütesiegel-Laufzeit auf dem neuesten Stand zu halten.

Zu beachten ist, dass nur Änderungen an den zertifizierten Produktbestandteilen relevant sind. In einem Teil der bisher vorgenommenen Zertifizierungen fallen der Zertifizierungsgegenstand (d. h. das „Produkt“ im Sinne der Zertifizierung) und der als „Produkt“ wahrgenommene Gegenstand auseinander: So werden häufig nur sicherheitsrelevante Komponenten einer Software zertifiziert, aber in Verkehrskreisen die gesamte Software als Produkt wahrgenommen.

2 Veränderung der Anforderungen

Teile der fortschreitenden technischen und rechtlichen Entwicklung schlagen sich in einer Änderung des Anforderungskataloges für Produkte nieder, der vom ULD fortgeschrieben wird. In die Fortentwicklung des Kataloges können zukünftig auch Protection Profiles und Schutzprofile einfließen, die mit anderen Zertifizierungsinstanzen abgestimmt werden, um so die Vergleichbarkeit verschiedener Gütesiegel zu schaffen.

Andere Änderungen werden nicht unmittelbar vom Anforderungskatalog erfasst, sondern ergeben sich durch Änderungen von Regelungen, auf die der Anforderungskatalog lediglich verweist. Dies sind beispielsweise Veränderungen von Datenkatalogen im materiellen Recht, die nicht unmittelbar und vollständig im Anforderungskatalog aufgeführt, aber von den Sachverständigen oder Prüfstellen[2] bei der Erstellung der Anforderungsprofile zu beachten sind.

Schließlich ergeben sich auch Änderungen im Bewertungsmaßstab für die Sachverständigen,

[1] Mit dem Begriff „ Antragsteller“ werden im Folgenden die Hersteller oder Vertriebsfirmen eines Produktes bezeichnet.

[2] Im Folgenden sind mit dem Begriff „Sachverständige“ ein oder zwei Sachverständige bzw. Prüfstellen gemeint, die zusammen für die beiden Bereiche Recht und Technik anerkannt sind.

damit die vom Produkt realisierten technischen Maßnahmen dem Stand der Technik entsprechen: Waren beispielsweise zum Zeitpunkt der Erstzertifizierung gewisse Schlüssellängen (noch) ausreichend, so mögen sie bei einer Rezertifizierung nicht mehr genügen. Auch andere technische Weiterentwicklungen können dazu führen, dass Sicherheitsmaßnahmen bereits zertifizierter Produkte bei einer Rezertifizierung den inzwischen gestiegenen Ansprüchen nicht mehr genügen.

3 Rezertifizierung nach Ablauf von zwei Jahren

Wenn ein Antragsteller mit einem aktuellen Datenschutz-Gütesiegel werben möchte, ist nach dem Ablauf der zweijährigen Laufzeit in jedem Fall eine Rezertifizierung erforderlich – es kommt nicht darauf an, ob das Produkt verändert wurde. Allerdings unterscheidet sich der Ablauf des Rezertifizierungsverfahrens je nach dem Ausmaß der Produktänderung.
Das ULD wird ca. 1 ½ Jahre nach Erteilung eines Gütesieges den Antragsteller auf den bevorstehenden Auslauf des Gütesiegels und die Möglichkeit der Rezertifizierung hinweisen.

3.1 Unverändertes Produkt

Wurde das Produkt nicht verändert, sondern ist dieses gegenüber dem zertifizierten Prüfmuster „baugleich“ geblieben, so beauftragt der Antragsteller Sachverständige mit der erneuten Prüfung des Produktes einschließlich der Produktdokumentation. Die Verwendung bestehender Unterlagen, z. B. aus dem ursprünglichen Zertifizierungsverfahren, ist möglich. Die Sachverständigen prüfen und aktualisieren ggf. das Anforderungsprofil hinsichtlich eventuell erfolgter Änderungen des Anforderungskataloges, gesetzlicher Änderungen (z. B. Datenprofile) sowie hinsichtlich des Standes der Technik (s. Abschnitt 2). Auf dieser Basis ist dann eine Neubewertung des Produktes vorzunehmen. Bei positivem Ergebnis stellt der Antragsteller einen Antrag auf Rezertifizierung an das ULD, das nach erfolgreicher Schlüssigkeitsprüfung des Gutachtens das Siegel für die Dauer von zwei weiteren Jahren erteilt.

3.2 Verändertes Produkt

Sollte das Produkt gegenüber der zertifizierten Prüfversion verändert worden sein, legt der Antragsteller dem von ihm beauftragten Sachverständigen das veränderte Produkt, die aktualisierte Dokumentation sowie zusätzlich eine Aufstellung der Veränderungen (Synopse) vor. Die Aufstellung vorgenommener Veränderungen soll den Prüfprozess beschleunigen. Kann der Antragsteller eine solche Aufstellung den Sachverständigen nicht vorlegen, so steigt der Aufwand der Sachverständigen: Es muss erneut eine vollständige Begutachtung erfolgen, da Produktänderungen in allen Bereichen, die hinsichtlich der Vorschriften über den Datenschutz und die Datensicherheit relevant sind, erfolgt sein können. Ein Ausschlusskriterium für eine Rezertifizierung ist das Fehlen einer solche Aufstellung nicht, ein Fehlen wird vor allem kostenrelevant sein. Auf die Zertifizierung eines Vorgängerproduktes ist im Antrag hinzuweisen.

Die Sachverständigen aktualisieren die Anforderungsprofile im Hinblick auf geänderte Anforderungskataloge sowie in rechtlicher und technischer Hinsicht und bewerten das Produkt anhand der Profile neu. Es folgt der Antrag auf Rezertifizierung beim ULD und bei erfolgreicher Schlüssigkeitsprüfung die Erteilung des Datenschutz-Gütesiegels für die Laufzeit von zwei Jahren.

4 Rezertifizierung vor Ablauf von zwei Jahren

Situationen, die eine Rezertifizierung erforderlich machen, können auch schon während der zweijährigen Laufzeit eintreten. Beispiele dafür sind Änderungen und Erweiterungen des geplanten Einsatzbereiches über den zertifizierten Bereich hinaus, tiefgreifende technische Entwicklungen oder Änderungen gesetzlicher Regelungen und schließlich Änderungen und Verbesserungen des Produktes. Aber nicht jede Änderung macht eine Rezertifizierung erforderlich: Sind bestimmte Erheblichkeitsschwellen (s. Abschnitt 4.3) nicht überschritten, so kann mit der Rezertifizierung bis zum Ende der regulären Gültigkeit gewartet werden.

4.1 Gründe für Rezertifizierung

Produktänderungen und -erweiterungen, Fehlerkorrekturen und Verbesserungen

Häufig werden während des Lebenszyklus des Produktes technische Änderungen, Verbesserungen oder Fehlerkorrekturen vorgenommen und im Rahmen neuer Versionen, als geänderte Verfahrensweisen, als Updates oder Sicherheitspatches bereitgestellt.

Änderung oder Erweiterung des Einsatzgebietes

Die Änderung oder Erweiterung des Einsatzgebietes für ein Produkt wird häufig zu einer Rezertifizierung (oder Ergänzung der ursprünglichen Zertifizierung) führen, weil in hinzukommenden Einsatzgebieten in aller Regel andere datenschutzrechtliche Regelungen gelten als im zertifizierten Einsatzbereich. Da die Produktdokumentation auch die hinzukommenden Einsatzgebiete beschreiben muss, führt jede Änderung oder Erweiterung des Einsatzgebietes zu einer Veränderung der Dokumentation und damit zu einer Änderung des Produktes selbst (da der Produktbegriff auch die Dokumentation umfasst).

Änderungen von technischen oder rechtlichen Grundlagen

Weitere Gründe, die eine Rezertifizierung erforderlich machen können, sind tiefgreifende Änderungen gesetzlicher Regelungen (beispielsweise die Kürzung von Datenkatalogen oder Übermittlungsverbote). Aber auch technische Entwicklungen, etwa der Bruch eines Kryptoalgorithmus, können einen Handlungsbedarf auslösen, weil dann das Produkt nicht mehr dem Stand der Technik entspricht.

Der Antragsteller der letzten Zertifizierung trägt die Verantwortung dafür, dass er erhebliche Veränderungen der für sein Produkt einschlägigen Rechtsvorschriften sowie der Technik als Handlungsbedarf erkennt. Erkennt er Handlungsbedarf, so richtet sich sein weiteres Vorgehen nach dem Verfahren für die Rezertifizierung vor Ablauf von zwei Jahren.

In aller Regel werden Antragsteller aus eigenem Interesse oder Kundenwünschen folgend auf diese rechtlichen oder technischen Änderungen eingehen und an ihrem Produkt Veränderungen vornehmen, die sie im Rahmen einer neuen Version oder als Updates oder Patches bereitstellen. Für den Zeitpunkt einer Produktänderung spielt auch eine Rolle, ob und welche Übergangsfristen bei rechtlichen Änderungen eingeräumt werden.

Sollte das ULD im Ausnahmefall Veränderungen eines zertifizierten Produktes für dringend geboten halten, räumt das ULD dem Betroffenen eine angemessene Frist zur Detailprüfung dieser Frage durch Sachverständige, zur Vornahme der erforderlichen Änderungen durch den Antragsteller sowie der Durchführung der Begutachtung ein; bis zum Ablauf dieser Frist darf das Siegel weiter ohne Einschränkung geführt werden.
Das ULD wird bei der Entscheidung, ob Produkte aufgrund einer Änderung rechtlicher oder technischer Grundlagen noch vor Ende der regulären Laufzeit geändert werden müssen, Erheblichkeitsschwellen zu Grunde legen. Daneben werden die Länge der Restlaufzeit des Gütesiegels sowie ggf. Übergangsfristen bei Änderungen rechtlicher Grundlagen in Betracht gezogen.

4.2 Ablauf des Verfahrens

In den meisten Fällen wird das Produkt innerhalb der Laufzeit geändert und ist damit nicht mehr „baugleich“ zu der bereits zertifizierten Version. Auch die Änderung des Einsatzgebietes wirkt sich auf die Dokumentation aus und verändert damit das Produkt. Die Vorgehensweise in diesen Fällen wird in Abschnitt 4.2.1 beschrieben. Führen Änderungen rechtlicher oder technischer Grundlagen zu einer Anpassung des Produktes, so kommt ebenfalls Abschnitt 4.2.1 zum Tragen.

Schließlich besteht die Möglichkeit, dass sich Änderungen rechtlicher oder technischer Grundlagen nicht in einer Änderung des Produktes durch den Antragsteller niederschlagen. Ob das Produkt weiterhin das Gütesiegel tragen kann (z. B. im Rahmen von Übergangsfristen oder weil Erheblichkeitsschwellen nicht überschritten sind), oder ob das ULD den Antragsteller zu einer Anpassung des Produktes auffordert, regelt sich nach Abschnitt 4.2.2.

Pauschale Aussagen, welche Änderungen eine Rezertifizierung erfordern, lassen sich nicht treffen. Die Entscheidung, ob nach einer Produktänderung eine Rezertifizierung notwendig ist, fällt in einem dreistufigen Prozess in Zusammenarbeit zwischen Antragsteller, den Sachverständigen und dem ULD.

4.2.1 Änderung des Produktes oder des Einsatzgebietes

Die Änderungen eines Produktes können ganz unterschiedliche Ausmaße haben. Auch ihr Einfluss auf die Verträglichkeit des Produktes mit den Vorschriften über Datenschutz und Datensicherheit kann stark variieren: So wird die Korrektur von Rechtschreibfehlern in Bearbeitungsmasken die Vorschriften über den Datenschutz und die Datensicherheit kaum tangieren. Die Umbenennung oder Erweiterung von Datenfeldern bei einer Eingabemaske für Datenbanken kann aber sehr wohl dazu führen, dass unzulässige Datenerhebungen vorgenommen werden. Eine ähnliche Bandbreite können auch technische Änderungen, etwa die Installation zusätzlicher Treiberprogramme, aufweisen: Während ein neuer Bildschirm- oder Druckertreiber unschädlich sein dürfte, kann die Installation einer neuen, für alle Benutzer verfügbaren Schnittstelle zu USB-Speichersticks die Datensicherheit stark gefährden. Nur solche Produktänderungen, die Vorschriften über Datenschutz- und Datensicherheit in starken Maße tangieren, begründen die Notwendigkeit einer Rezertifizierung; unterhalb einer gewissen „Bagatellgrenze“ können Änderungen im Hinblick auf die zweijährige Laufzeit toleriert werden. Es sind zwei Konstellationen denkbar:

4.2.1.1 Konstellation 1: Produktänderungen, die Datenschutz und Datensicherheit nicht berühren

Das Produkt wird kaum verändert, ist aber nicht mehr „baugleich“ mit der geprüften Version. Die Veränderungen tangieren die Vorschriften über den Datenschutz und die Datensicherheit **nicht**. In diesem Fall ist **keine** Rezertifizierung erforderlich. Die Laufzeit des erteilten Gütesiegels endet regulär.

Die Feststellung über die Relevanz der Veränderung liegt in der Hand des Antragstellers bzw. der Vertriebsfirma. Diese haben dabei eine besondere Verantwortung, denn sie sind zunächst die Einzigen, die von einer Änderung des Produktes Kenntnis haben, das Zusammenspiel unterschiedlicher Produktkomponenten kennen und sicherheitstechnische Wechselwirkungen innerhalb des Produktes einschätzen können.

Berühren hingegen die vorgenommenen Änderungen die Vorschriften über den Datenschutz und die Datensicherheit oder bestehen beim Antragsteller darüber Unsicherheiten, ist ein Sachverständiger einzuschalten. Dies wird im folgenden Abschnitt beschrieben.

4.2.1.2 Konstellation 2: Produktänderungen mit Einfluss auf den Datenschutz und die Datensicherheit

Das Produkt ist nicht mehr „baugleich“ mit der geprüften Version; die Veränderungen tangieren die Vorschriften über den Datenschutz und die Datensicherheit. In Zusammenarbeit mit Sachverständigen und dem ULD ist zu überprüfen, ob eine Rezertifizierung notwendig ist. Dies ist der Fall, wenn die vorgenommenen Änderungen erhebliche Ausmaße haben.

Der Antragsteller stellt zunächst selbst fest, dass die Produktänderungen die Vorschriften über Datenschutz und Datensicherheit tangieren, und nimmt Kontakt zu Sachverständigen auf. Er legt das veränderte Produkt mit der fortgeschriebenen Dokumentation sowie einer Aufstellung der Veränderungen (Synopse) vor. Die Sachverständigen stellen das Ausmaß der Veränderung fest und entscheiden, ob die vom ULD formulierten **Erheblichkeitsschwellen** für die Rezertifizierung unterschritten oder überschritten werden (vgl. Abschnitt 4.3).

Unterschreiten der Erheblichkeitsschwellen:

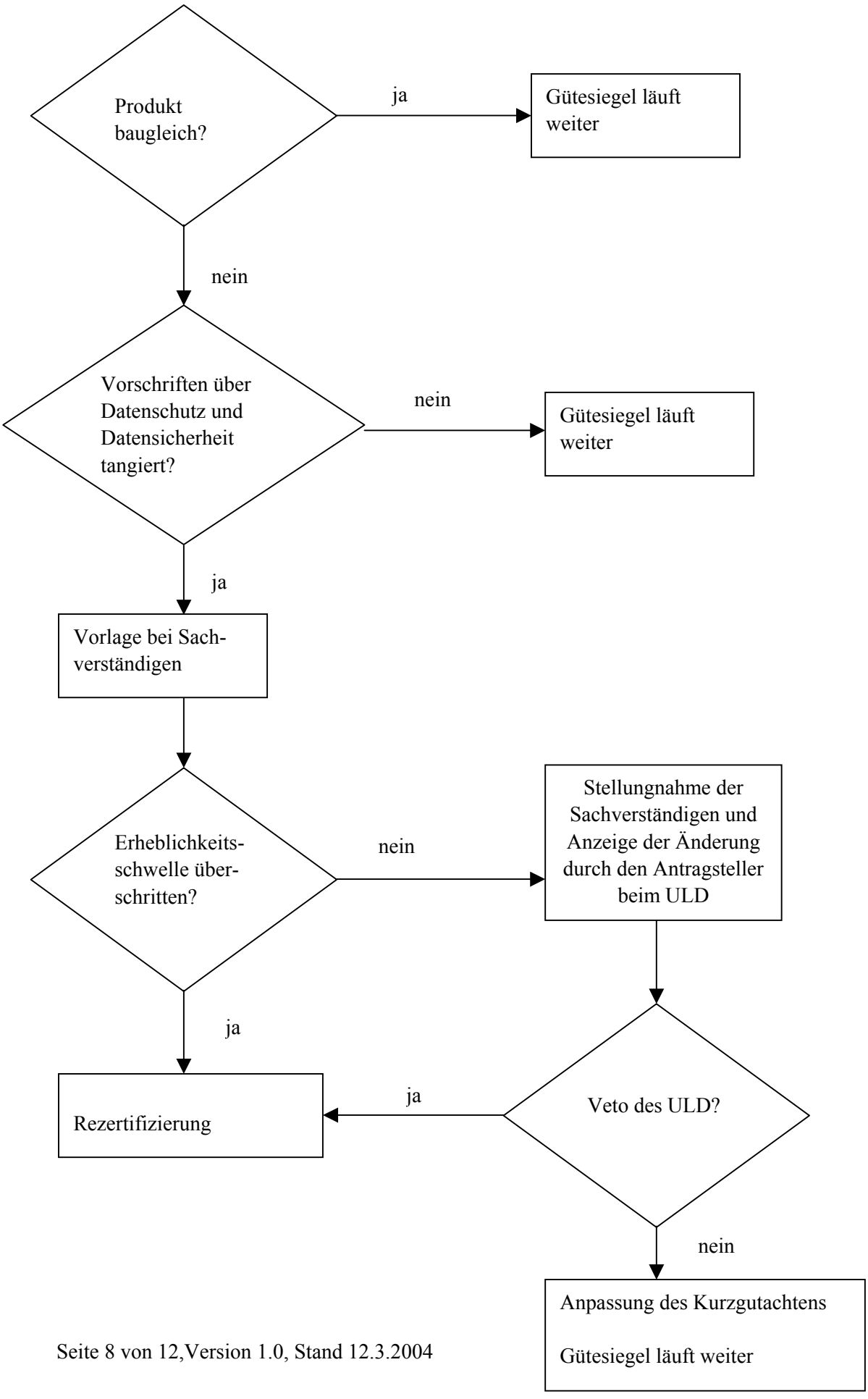
Werden die Erheblichkeitsschwellen unterschritten, erstellen die Sachverständigen eine schriftliche Stellungnahme. Der Antragsteller zeigt dem ULD die Veränderung des Produktes unter Vorlage der gutachterlichen Stellungnahme an. Legt das ULD innerhalb einer Frist von zwei Monaten nach Eingang der Vorlage gegen die Bewertung der Sachverständigen kein Veto ein, so läuft die Zweijahresfrist des Datenschutz-Gütesiegels weiter. Legt das ULD im Ausnahmefall sein Veto ein, so ist das Rezertifizierungsverfahren (s. Abschnitt 3.2) einzuleiten.

Überschreiten der Erheblichkeitsschwellen:

Überschreiten die im Produkt vorgenommenen Veränderungen nach der Einschätzung der Sachverständigen die Erheblichkeitsschwellen des ULD, so ist das Verfahren zur Rezertifizierung (s. Abschnitt 3.2) einzuleiten; das Siegel wird am Ende des neuen Verfahrens für den vollen Zeitraum von zwei Jahren erteilt.

Auf der folgenden Seite ist der Ablauf schematisch zusammengefasst.

Ablaufschema der Rezertifizierung bei Änderung des Produktes



4.2.2 Änderungen rechtlicher oder technischer Grundlagen mit Einfluss auf den Datenschutz und die Datensicherheit

Die Veränderungen rechtlicher oder technischer Grundlagen tangieren die Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit. Vermutet der Antragsteller einen Handlungsbedarf, so ist in Zusammenarbeit mit den Sachverständigen zu überprüfen, ob eine Produktanpassung und eine nachfolgende Rezertifizierung notwendig sind. Dies ist der Fall, wenn die Änderungen der rechtlichen oder technischen Grundlagen erhebliche Ausmaße haben. Sofern nicht der Antragsteller bereits tätig geworden ist, kann das ULD diesen Sachverhalt überprüfen und den Antragsteller zur Prüfung und ggf. zur Anpassung des Produktes auffordern.

Der Antragsteller der letzten Zertifizierung trägt die Verantwortung dafür, dass er erhebliche Veränderungen der für sein Produkt einschlägigen Rechtsvorschriften sowie der Technik als Handlungsbedarf erkennt. Erkennt oder vermutet er Handlungsbedarf, so nimmt er Kontakt zu den Sachverständigen auf. Die Sachverständigen stellen das Ausmaß der Veränderung fest und entscheiden, ob die vom ULD formulierten **Erheblichkeitsschwellen** überschritten werden (vgl. Abschnitt 4.3).

Unterschreiten der Erheblichkeitsschwellen:

Werden die Erheblichkeitsschwellen unterschritten, erstellen die Sachverständigen eine schriftliche Stellungnahme. Der Antragsteller zeigt dem ULD unter Vorlage der gutachterlichen Stellungnahme an, dass das baugleiche Produkt weiterhin die Vorschriften über Datenschutz und Datensicherheit erfüllt. Legt das ULD innerhalb einer Frist von zwei Monaten nach Eingang der Vorlage gegen die Bewertung der Sachverständigen kein Veto ein, so läuft die Zweijahresfrist des Datenschutz-Gütesiegels weiter.

Legt das ULD im Ausnahmefall ein Veto ein, so fordert das ULD den Antragsteller zu einer Änderung des Produktes auf. Dieser Fall ist im folgenden Abschnitt beschrieben.

Überschreiten der Erheblichkeitsschwellen:

Überschreiten die im Produkt vorgenommenen Veränderungen nach der Einschätzung der Sachverständigen die Erheblichkeitsschwellen des ULD oder legt das ULD ein Veto gegen die Bewertung der Sachverständigen ein (s. o.), so ist der Antragsteller aufgefordert, sein Produkt an die geänderten technischen und rechtlichen Grundlagen anzupassen und eine Rezertifizierung (s. Abschnitt 3.2) einzuleiten; das Siegel wird am Ende des Verfahrens für den vollen Zeitraum von zwei Jahren erteilt.

4.3 Erheblichkeitsschwellen

Die exakte Definition eines Schwellenwertes, dessen Überschreiten eine Rezertifizierung notwendig macht, wird angesichts der Vielzahl unterschiedlicher IT-Produkte kaum möglich sein. Eine sinnvolle Lösung kann daher nur die Annäherung mit Hilfe von Beispielen unterschiedlicher Erheblichkeitsschwellen sein, bei deren Überschreiten ein Rezertifizierungsprozess eingeleitet werden muss.

Die folgenden Beispiele für eine Überschreitung der Erheblichkeitsschwellen sind danach strukturiert, ob

- Änderungen des Produktes,
- Änderungen des Einsatzgebietes des Produktes oder
- Änderungen der rechtlichen oder technischen Grundlagen

vorliegen.

4.3.1 Änderungen des Produkts

Änderungen des Produktes oder seines Einsatzbereiches bzw. Veränderungen rechtlicher oder technischer Rahmenbedingungen sind immer Anlass, die Erforderlichkeit einer Rezertifizierung zu prüfen. Allerdings kann es Änderungen geben, die von geringem Umfang sind und keine Auswirkungen bezüglich der Rechtskonformität mit den relevanten Datenschutzvorschriften haben, so dass von einer Rezertifizierung abgesehen werden kann. In den meisten Fällen ist aber zu prüfen, ob die Änderungen die Erheblichkeitsschwellen überschreiten:

Anzeichen für überschrittene Erheblichkeitsschwellen

Obwohl die Vergabe von **Versionsnummern** in der IT-Branche an keinerlei festgelegtes Schema gebunden ist, kann in der Regel davon ausgegangen werden, dass bei einer Änderung der Versionsnummer eine Rezertifizierung erforderlich ist. In jedem Fall sei es dem Antragsteller in diesen Fällen nahe gelegt, die Notwendigkeit einer Rezertifizierung durch Sachverständige überprüfen zu lassen.

Bei **Akkumulation** von kleineren Fortschreibungstätigkeiten, Patches oder Updates des Produktes, die über einen längeren Zeitraum hinweg insgesamt die Funktion des Produkts ändern oder erweitern oder offensichtlich von datenschutzrechtlicher Relevanz sind, ist ebenfalls von der Notwendigkeit einer Rezertifizierung auszugehen. Beispielsweise wäre es möglich, dass mehrere Patches oder Updates, die für das Produkt entwickelt werden (und z. B. lediglich der Stabilität oder Verfügbarkeit dienen), jeweils für sich gesehen nicht die Erheblichkeitsschwelle für Änderungen überschreiten, also jeweils auch kein Rezertifizierungsverfahren initiiert werden muss. Wohl aber kann sich aus der **Gesamtsicht** auf die Änderungen im Rahmen der Produktpflege, die ein Antragsteller in Form eines Change- bzw. Maintenance-Managements üblicherweise vornimmt, die Notwendigkeit einer Rezertifizierung ergeben.

Funktionsänderungen bzw. -erweiterungen des Produktes, die datenschutzrechtlich relevant sind (z. B. die Implementierung neuer Schnittstellen und Übertragungsmöglichkeiten zu Dritten), machen in jedem Fall eine Rezertifizierung notwendig.

Auch **Änderungen der (technischen) Sicherheitseigenschaften** des Produkts (z.B. Änderungen des Verschlüsselungsverfahrens, der verwendeten Schlüssellängen, des Authentisierungsverfahrens, der implementierten Mindestanforderungen an Passwörter, der Administration, der Sicherung, des Backups usw.) sind ein starkes Indiz dafür, dass eine Rezertifizierung notwendig ist. Lediglich bei technischen Änderungen, die zweifelsfrei einer Erhöhung der Datensicherheit dienen (wie dies z. B. bei einer Vergrößerung der implementierten Mindestlänge von Passwörtern oder von Schlüssellängen nahe liegt), genügt eine Überprüfung durch die Sachverständigen und die Anzeige einer Änderung beim ULD.

Ebenso sind **Änderungen von Vertragsbedingungen**, die datenschutzrechtliche Verantwortlichkeiten bei Verfahren betreffen (etwa Kontrollrechte im Rahmen der Auftragsdatenverarbeitung), Anlass für eine Rezertifizierung.

4.3.2 Änderungen des Einsatzgebietes des Produktes

Eine Änderung des Einsatzgebietes des Produktes schlägt sich in der Produktdokumentation und damit im Produkt nieder. Sie macht in der Regel auch das Heranziehen weiterer bzw. anderer gesetzlicher Grundlagen erforderlich. Daher ist die Erheblichkeitsschwelle überschritten und eine Rezertifizierung notwendig.

4.3.3 Änderungen der Grundlagen eines Produktes

Änderung rechtlicher Grundlagen

Wenn sich gesetzliche Grundlagen ändern, ist diesem Schritt bereits eine intensive Kontextdiskussion vorausgegangen, so dass man davon ausgehen kann, dass die hieraus resultierenden Änderungen in IT-Produkten sich an mehreren Stellen intensiv auswirken. Nur in seltensten Fällen dürfte es sich um geringfügige Änderungen, wie z. B. den Wegfall eines einzelnen Datenfeldes, handeln. Daher wird die Erheblichkeitsschwelle in der Regel überschritten sein.

Änderung technischer Grundlagen

Der **Stand der Technik** wird sowohl in der IT als auch in anderen technischen Bereichen als ein Grenzwert angesehen, der durch Publikationen vorgegeben wird und in der Fachwelt dadurch als Konsens gesichert wird. Er kann bei Fachleuten als bekannt vorausgesetzt werden.

Ein Indiz für eine **erhebliche Änderung** der Grundlagen ist, wenn ein unverändertes Produkt unter den geänderten Grundlagen nicht gütesiegelfähig wäre und Produktänderungen in einem Ausmaß oberhalb der Erheblichkeitsschwelle notwendig wären, damit das Produkt die Vorschriften über Datenschutz und Datensicherheit erfüllt. Dies ist z. B. der Fall, wenn sich in Verschlüsselungsverfahren **systembedingte Schwächen** zeigen, die die Vertraulichkeit von Daten akut gefährden. Ändern sich lediglich Empfehlungen zur mittelfristigen Länge von Schlüsseln, so kann das Produkt mit Rücksicht auf die Restlaufzeit von höchsten zwei Jahren unverändert bleiben.

5 Hinweise für Antragsteller

5.1 Hinweise zur Vertragsgestaltung mit Sachverständigen

Im Fall einer Rezertifizierung ist es für Sachverständige hilfreich, auf bereits bestehende Unterlagen vorangegangener Zertifizierungen zurückzugreifen. Dies betrifft z. B. Unterlagen der Produktdokumentation und erstellte Anforderungsprofile. Im Rahmen der Verträge mit Sachverständigen sollte daher die Frage geklärt werden, welche Rechte Antragsteller und Sachverständige an den entsprechenden Unterlagen haben.

5.2 Synopse

Soll ein verändertes Produkt rezertifiziert werden, so ist eine Zusammenstellung der vorgenommenen Änderungen für den Rezertifizierungsprozess hilfreich, weil es den Aufwand für Sachverständige und das ULD verringert (siehe auch Abschnitt 3.2). Hersteller sollten schon während der Änderung und Anpassung von Produkten (einschließlich der Dokumentation) eine solche Aufstellung erstellen, z. B. im Rahmen eines Versionsmanagements, denn eine nachträgliche Zusammenstellung erfolgter Änderung ist erfahrungsgemäß kostenintensiver als eine begleitende Erstellung. Auch für die Beurteilung der Frage, ob akkumulierende Änderungen in der Gesamtsicht eine Rezertifizierung erforderlich machen (siehe Abschnitt 4.3.1), ist eine solche Aufstellung erforderlich.

5.3 Kosten

Die Kosten für eine Rezertifizierung setzen sich zusammen aus den frei aushandelbaren Kosten für die Begutachtung durch Sachverständige sowie aus Gebühren des ULD. Es ist davon auszugehen, dass der Aufwand und damit auch die Kosten einer Begutachtung durch die sachverständigen im Rezertifizierungsfall geringer sind als bei einer Erstzertifizierung. Dies dürfte wesentlich davon abhängen, welche Unterlagen der Antragsteller den Sachverständigen zur Verfügung stellen kann (siehe dazu auch die vorherigen Abschnitte).

Die Gebühren des ULD werden im Rahmen der Gebührensatzung festgelegt. Wie bei Erstzertifizierungen sind sie aufwandsabhängig. Die Gebührensätze für die Rezertifizierung werden etwa bei der Hälfte der Kosten für eine Erstzertifizierung liegen.