Datenschutz mit Gütesiegel

Einleitung

Ein Ende des technologischen Fortschritts ist nicht in Sicht. Neben den gewünschten Verbesserungen und Erleichterungen des täglichen Lebens sowie der dadurch erzielten wirtschaftlichen Effizienzen, die dadurch erzielt werden, sollte darauf geachtet werden, dass der Mensch nicht auf der Strecke bleibt. Der Mensch, als ein mit Persönlichkeitsrechten versehenes Individuum, darf nicht bloßes Objekt der Informationstechnologie werden. Technik kann nur solange gut sein, solange sie durch den Menschen beherrschbar bleibt. Auch hier kommt George Orwell's „Doublethink: Freedom is Slavery“ zum Tragen: wir denken, dass uns der Technikeinsatz das Leben leichter macht, gerade dies ist aber oft nur eine Illusion und wir machen uns, ohne es zu merken, selbst zu Sklaven unserer eigenen technologischen Entwicklungen. Aus diesem Grunde ist wichtig, dass dem Datenschutz ein entsprechend hoher Stellenwert eingeräumt wird.

Allgemeines

Datenschutz und Technik schließen sich jedoch nicht aus. Datenschutzgerechte Technologien tragen gerade dem Gedanken Rechnung, dass die Beachtung der Persönlichkeitsrechte des Einzelnen unverzichtbar ist. Zu den wichtigsten Kriterien gehören: der Grundsatz der Datenvermeidung und Datensparsamkeit, der Einsatz von technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten sowie die Berücksichtigung der Rechte der Betroffenen insbesondere auf Auskunft, Benachrichtigung, Datenberichtigung, -löschung und -sperrung.

Ob der Einsatz einer Software datenschutzkonform erfolgen kann, wird im Rahmen einer Zertifizierung überprüft. Das Datenschutz-Gütesiegel dokumentiert dies nach außen. Unter Zertifizierung versteht man im Allgemeinen die Überprüfung von Verfahren durch eine unabhängige Behörde, die über eine besondere Fachkunde verfügt. Prüfungsgrundlage ist ein Katalog von Anforderungen, der bei jeder Prüfung standardmäßig herangezogen wird. Das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH) ist eine solche unabhängige Zertifizierungsstelle.

Im Folgenden wird das Datenschutz-Gütesiegel des ULD SH vorgestellt. Andere Zertifizierungsstellen für Datenschutz-Gütesiegel, sind der Verfasserin nicht bekannt.

Warum Zertifizierung?

Die Zertifizierung bringt dem Hersteller des IT-Produktes Wettbewerbsvorteile, denn er kann sich dadurch maßgeblich von anderen Mitbewerbern abheben. Auch die Akzeptanz des Produktes bei Verbrauchern wird dadurch erhöht, da der Verbraucher darauf vertrauen kann, dass beim Einsatz eines solchen Produktes mit seinen personenbezogenen Daten sorgsam umgegangen wird. Dieser Aspekt ist nicht hoch genug zu bewerten, da die Angst vor Datenmissbrauch das größte Hemmnis des eCommerce darstellt.

Das Datenschutz-Gütesiegel des ULD SH erleichtert auch den Einsatz von IT-Verfahren in der **öffentlichen Verwaltung**. So sieht insbesondere das schleswig-holsteinische Landesdatenschutzgesetz explizit vor, dass vorrangig zertifizierte Software-Produkte in den Behörden eingesetzt werden sollen. Das Gütesiegel kann deshalb für ein Unternehmen auch bei

öffentlichen Ausschreibungen von Vorteil sein. Gerade in Schleswig-Holstein wird das Gütesiegel zwingend berücksichtigt.

Mit Ausnahme von Brandenburg sind die Verwaltungen der anderen Bundesländer nicht gehalten, ein Gütesiegel des ULD SH zu berücksichtigen. Es gibt zwar teilweise auch dort Bestrebungen zertifizierte Produkte bevorzugt zu behandeln, das ULD SH Gütesiegel wird jedoch nicht vorbehaltlos anerkannt. Die **Anerkennung des Gütesiegels** in anderen Bundesländern hängt davon ab, ob das jeweilige Landesdatenschutzgesetz abweichende Regelungen enthält und ob diese durch das IT-Verfahren eingehalten werden. In der Regel unterscheiden sich die einzelnen Landesdatenschutzgesetze kaum. Eventuelle Abweichungen können anhand des veröffentlichten Kurzgutachtens kostensparend und einfach aufgedeckt und eventuelle Ergänzungen bzw. Änderungen vorgenommen werden, um das Produkt in der jeweiligen Behörde einsetzen zu können. Im Übrigen können landesspezifische Datenschutzvorschriften bereits im Gutachten berücksichtigt werden, wenn der Hersteller zum Zertifizierungszeitpunkt bereits weiß in welchem Bundesland er das Produkt in Behörden einsetzen möchte.

Das Datenschutz-Gütesiegel des ULD SH wird auch Produkten verliehen, die ausschließlich im **nichtöffentlichen Bereich** eingesetzt werden. Aus dem Register der zertifizierten Produkte beim ULD SH ergibt sich, dass auch vielen Verfahren, die für den Einsatz im privaten Bereich konzipiert sind, bereits ein Gütesiegel verliehen wurde. Als Beispiele können dabei eine Software Applikation für digitale ärztliche Diktate sowie eine webbasierte Anwendung für berufsvorbereitende Bildungsmaßnahmen genannt werden.

Zertifizierungsverfahren beim ULD SH

Jedes Unternehmen unabhängig vom Firmensitz kann einen Zertifizierungsantrag stellen. Gegenstand der Zertifizierung ist die Vereinbarkeit des Produktes mit den Anforderungen an den Datenschutz und an die Datensicherheit. Die Zertifizierungsvorbereitung erfolgt durch einen oder mehrere Gutachter, die am ULD SH als Sachverständige akkreditiert sind. Diese erstellen ein Gutachten, das aus einem rechtlichen und einem technischen Teil besteht. Nach bestandener Überprüfung des Gutachtens durch das ULD SH erfolgt die Zertifizierung durch den Erlass eines Zertifizierungsbescheides. Das Gütesiegel wird i.d.R. zeitlich befristet auf zwei Jahre verliehen. Nach Ablauf dieses Zeitraums ist eine Rezertififzierung notwendig.

Zertifizierungsanforderungen

Das ULD SH hat einen Anforderungskatalog[1] erstellt, der aus vier Bausteinen besteht:

Anhand des ersten Bausteins wird geprüft, ob die technische Gestaltung die Grundsätze der **Datenvermeidung** und der **Datensparsamkeit** berücksichtigt hat. Wenn schon aufgrund des Einsatzzwecks die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten notwendig ist, stellt sich die Frage, ob die Daten früh gelöscht, anonymisiert oder pseudonymisiert werden können. Ferner wird auch hier geprüft, ob die Verarbeitung der personenbezogenen Daten transparent erfolgt. **Transparenz** erfordert, dass insbesondere die Produktbeschreibung leicht zu finden ist, der Datenfluss deutlich gemacht wird und die Daten auf dem aktuellen Stand sind.

Im zweiten Baustein wird geprüft, ob die Verarbeitung der Daten **rechtmäßig** erfolgt. Im Vorfeld muss der Gutachter anhand der zu speichernden Datenarten bereits die einzelnen datenschutzrelevanten Verfahren definiert haben. Angelehnt an den datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt wird zunächst geprüft, ob eine gesetzliche Ermächtigungsgrundlage vorliegt, dann ob die Möglichkeit besteht, eine Einwilligung wirksam abzufragen. Die Wirksamkeitsvoraussetzungen einer Einwilligung werden hier eingehend geprüft. Ferner werden Besonderheiten berücksichtigt, wie die Verarbeitung besonderer personenbezogener Daten, die Übermittlung von Daten und die Frage, ob und wie die Löschung der Daten nach dem Wegfall des Erhebungszwecks bewerkstelligt wird. Die allgemeinen Datenschutzgrundsätze: Zweckbindungs- und Trennungsgrundsatz sind auch Bestandteile des zweiten Prüfungsbausteins. Sollte eine Auftragsdatenverarbeitung vorgesehen sein, wird untersucht, ob der Einsatz externer Dritter zulässig ist. Schließlich widmet sich der Gutachter auch der Prüfung besonderer technischer Datenverarbeitungsmaßnahmen, wie z.B. dem Einsatz von Systemen zur automatisierten Einzelentscheidung oder Videoüberwachungsmaßnahmen.

Der dritte Prüfungsschritt widmet sich den **technischen und organisatorischen Maßnahmen**, die zum Schutz der Betroffenen eingesetzt werden. Das sind folgende Maßnahmen entsprechend der Anlage zu § 9 BDSG:

- Zutrittskontrolle: Sicherstellung, dass Unbefugten der Zutritt zu den Systemen verwehrt wird, mit denen personenbezogene Daten verarbeitet oder genutzt werden

1 Vgl. für Einzelheiten: Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH

- Zugangskontrolle: Verhinderung, dass die Systeme von Unbefugten genutzt werden können (werden bspw. Authentisierungs-, Zugriffskontroll- und Verschlüsselungsmechanismen eingesetzt?)
- Zugriffskontrolle: Vorliegen eines Berechtigungskonzeptes, wonach gewährleistet werden soll, dass nur die Personen mit der entsprechenden Berechtigung Zugriff haben auf die Systembestandteile, die für sie bestimmt sind (werden Protokollierungen vorgenommen und wie wird mit den Protokolldaten verfahren?)
- Weitergabekontrolle: Gewährleistung, dass im Rahmen eines Datentransfers die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und, dass festgestellt werden kann, an welchen Empfänger die Daten übermittelt werden
- Eingabekontrolle: Sicherstellung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten eingegeben, verändert oder entfernt worden sind
- Auftragskontrolle: Sicherstellung, dass im Rahmen einer Auftragsdatenverarbeitung personenbezogene Daten entsprechend den Weisungen des Auftraggebers verarbeitet werden können
- Verfügbarkeitskontrolle: Schutz der personenbezogenen Daten gegen zufällige Zerstörung oder Verlust
- Trennungsgebot: Sicherstellung, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden auch getrennt verarbeitet werden können

Ferner wird untersucht, ob die Vorabkontrolle, die Erstellung von Verfahrensverzeichnissen sowie die Tätigkeit des Datenschutzbeauftragten unterstützt wird. Schließlich sind die technischen und organisatorischen Maßnahmen beim Einsatz besonderer Verfahren wie Chipkarten oder Videoüberwachung Gegenstand diese Prüfungsschrittes.

Die Einhaltung der **Rechte der Betroffenen** wird im vierten Baustein geprüft. Dabei fokussiert sich die Untersuchung darauf, ob das Softwareprodukt aufgrund seiner Gestaltung die Einhaltung der Rechte der Betroffenen ermöglicht bzw. unterstützt.

Für ausführliche Informationen zum Zertifizierungsverfahren wird auf den Internetauftritt des ULD SH unter www.datenschutzzentrum.de verwiesen.

Sigrid Wild LL.M.

Frau Wild berät als Rechtsanwältin Unternehmen in den Bereichen Datenschutz und EDV-Recht und ist anerkannte Sachverständige für IT-Produkte (rechtlich) beim ULD SH.