Datenschutz-Gütesiegel

Zunehmend verschaffen sich Unternehmen einen Wettbewerbsvorteil, die sich mit hoher Sorgfalt um Datenschutz kümmern. Das EuroPriSe Seal ist der nach außen sichtbare Beleg dafür.

WIEN – Die rasante Entwicklung ständig neuer IT-Technologien hat unsere Welt verändert. Täglich neue IT-Produkte und -services erhöhen unsere Lebensqualität. In gleicher Geschwindigkeit wird jedoch mehr und mehr unsere Privatsphäre bedroht.

Das EuroPriSe Seal ist ein europaweit anerkanntes Datenschutz-Gütesiegel. Die Initiative geht vom ULD, dem Unabhängigen Landeszentrum für Datenschutz in Schleswig Holstein aus. Dabei werden in einem 2-stufigen Zertifizierungs-Verfahren die zu zertifizierenden IT-Services und IT-Projekte geprüft. In der ersten Phase werden diese von dafür namentlich zugelassenen Experten auditiert. In der zweiten Phase werden die erstellten Prüfberichte von einer unabhängigen Datenschutzkommission im ULD geprüft. Erst danach wird das auf zwei Jahre zeitlich begrenzte Gütesiegel ausgestellt.

Im Moment läuft das Pilotprojekt in verschiedenen Mitgliedsstaaten der Europäischen Union wie Deutschland, Österreich, Großbritannien, Slowakei, Spanien und Schweden.

Das europäische Datenschutz-Gütesiegel – European Privacy Seal (EuroPriSe) – bestätigt, dass ein IT-Angebot in Vereinbarkeit mit europäischem Datenschutzrecht eingesetzt werden kann. Datenschutzrechtlich korrekte und technisch sichere Produkte, etwa Internet-Angebote aus dem Gesundheitsbereich oder bei der Kundendatenverarbeitung, sollen dadurch einen Wettbewerbsvorteil erhalten.

Die Prüfverfahren sind streng und die Prüfberichte genau reglementiert. Um sicherstellen zu können, dass der Schutz der Daten auch tatsächlich gewährleistet wird, müssen zahlreiche Kriterien erfüllt sein. So müssen alle verarbeiteten Daten gelistet werden, der Datenfluss muss exakt beschrieben werden, die in den Prozess eingebundenen Verarbeiter müssen offengelegt sein, die Vermeidung nicht erforderlicher Daten muss sichergestellt sein (Minimalprinzip) und es muss technisch und organisatorisch gewährleistet sein, dass Daten nicht unabsichtlich an Dritte gelangen. Dies wird durch jeweils einen technischen und einem juristischen Experten geprüft und dokumentiert.

Konkret bedeutet dies, dass in einem ersten Schritt zunächst einmal die Evaluierung der Produkte durch zugelassene technische und juristische Experten stattfindet. Dabei werden die grundsätzlichen Aspekte der Datenverarbeitung geprüft wie

– der Zweck der Verarbeitung
– die Liste der verarbeiteten Daten
– die Benennung des Auftraggebers
– das Vorliegen etwaiger internationaler Übermittlungen
– sowie Einhaltung der Prinzipien der Datenvermeidung und -minimierung.

Im zweiten Schritt geht es in die Details, ob etwa die Verarbeitung auf Grundlage einer Zustimmung der betroffenen Person oder aufgrund der Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erfolgt. Auch wird geprüft, ob die verarbeiteten Daten zweckentsprechend spezifiziert und eingeschränkt sind. Daneben wird gefragt, ob es Dienstleister in Drittstaaten (= Nicht-Mitgliedstaaten der EU) gibt und ob Daten an sie übermittelt werden. Es wird auch abgeklärt, ob ein Informationsverbundsystem oder andere spezielle Typen der Datenverarbeitung vorliegen und ob die erforderlichen Voraussetzungen vorliegen.

TECHNISCH-ORGANISATORISCHE BEGUTACHTUNG

Hier werden allgemeine technische Angaben gemacht. Etwa zur Verhinderung eines unerlaubten Datenzugriffs, zur Verwendung von Passwörtern, zur Netzwerksicherheit, zu den Backup-Regelungen oder zur Datenlöschung. Daneben wird einerseits die Verschlüsselung genau unter die Lupe genommen. Andererseits untersuchen die Experten eine etwaige Pseudonymisierung und Anonymisierung sowie die technischen Datensicherheitsmaßnahmen und die Datentransparenz. Sie kontrollieren, ob das geprüfte Produkt oder die Dienstleistung die Rechte der Betroffenen nach der EU-Datenschutzrichtlinie gewährleistet.

Erst wenn alle diese Voraussetzungen erfüllt sind und der streng reglementierte Auditbericht von der Expertenkommission im ULD akzeptiert wurde, wird das Europäische Datenschutz-Gütesiegel verliehen, das nach zwei Jahren wieder erneuert werden muss.

Zur Zeit sind europaweit sechs Unternehmen zertifiziert, zahlreiche Unternehmen durchlaufen gerade das Zertifizierungsverfahren, auch in Österreich, wo das Auditing von Herbert Bieber (BWsecure) gemeinsam mit dem Datenschutzexperten Rainer Knyrim durchgeführt wird. *[el]*

www.bwsecure.net

DER ZERTIFIZIERUNGSABLAUF IM ÜBERBLICK

1. Zunächst muss der Interessent einen rechtlichen und einen technischen Experten aus dem Pool der zertifi zierten Experten von EuroPriSe auswählen.
2. Nachdem die Experten kontaktiert wurden, wird mit ihnen eine Zertifizierungsvereinbarung geschlossen und die Evaluierungsschritte gemeinsam besprochen.
3. Im dritten Schritt sollte ein erster Kontakt mit dem ULD vereinbart werden. Er soll abklären, ob das Produkt oder die Dienstleistung aus Sicht von EuroPriSe überhaupt zertifizierungsfähig ist.
4. Die Experten prüfen danach entsprechend den Vorgaben des Katalogs die einzelnen Punkte der Evaluierung.
5. Dann muss die Zertifizierung beim ULD beantragt werden. Das entsprechende Formular ist online unter http://www.european-privacy-seal.eu abrufbar.
6. Der nächste Schritt ist, dass das EuroPriSe-Konsortium das IT-Produkt oder die IT-Dienstleistung für die Pilotzertifizierung zulässt.
7. Sind all diese Schritte erledigt, hat der Hersteller des Produkts die Zertifizierungsvereinbarung mit den Experten, den Evaluierungsreport sowie einen kurzen öffentlichen Bericht beim ULD einzureichen.
8. Jetzt prüft das ULD den Expertenbericht und entscheidet, ob das Gütesiegel überreicht werden kann oder nicht.