Das xDSB Datenschutz Gütesiegel

Vergaberichtlinien für die Vergabe des Gütesiegels
„xDSB Datenschutz geprüft“
im Folgenden: „Gütesiegel“

Stand August 2016

Herausgeber: xDSB Datenschutz
Greschbachstraße 6a
76229 Karlsruhe

Alle Rechte an dem Gütesiegel und der Vergaberichtlinien liegen beim Herausgeber

Für die Vergabe des Gütesiegels existieren strenge Vorgaben.

Das Gütesiegel ist Zeichen eines etablierten
Datenschutzmanagements eines Unternehmens.

Durch die Vergabe des Gütesiegels soll Kunden und Mitarbeitern eines Unternehmens oder sonstige von einer Datenverarbeitung betroffenen Personen die Sicherheit gegeben werden, dass mit seinen personenbezogenen Daten in diesem Unternehmen sorgsam und unter Beachtung der Datenschutzvorschriften umgegangen wird.

Das Gütesiegels darf vom Unternehmen oder Dritten weder in Form noch Farbe verändert werden.

(Muster)

Inhalt

Allgemeines

Mit Vergabe des xDSB Datenschutz Gütesiegels dokumentiert xDSB Datenschutz, dass das geprüfte Unternehmen in dem im Gütesiegel verzeichneten Kalenderjahr ein mindestens weitgehend rechtskonformes Datenschutzmanagement betreibt oder betrieben hat.

Vor Vergabe des Gütesiegels findet eine ausführliche datenschutzrechtliche Überprüfung der datenschutzrechtlich relevanten Prozesse des Unternehmens statt, welche in einem sog. internen Verfahrensverzeichnis dokumentiert sind.

xDSB Datenschutz berät seit 2005 Unternehmen im Datenschutz, Datenschutzmanagement und der Datensicherheit.

Auditierungen werden in der Regel von dem
EDV-Sachverständigen (BVFS) und TÜV-Datenschutzauditor Michael Bätzler durchgeführt.

Datenschutzrechtliche Beratungen führt ausschließlich Rechtsanwalt Thomas Steinle, LL.M., Fachanwalt für Informationstechnologierecht, durch.

Was wird geprüft

Das Gütesiegel wird nach erfolgreicher Prüfung des Datenschutzmanagements eines Unternehmens vergeben. Hierbei werden die nach BDSG grundlegend erforderlichen Mindestanforderungen an das Datenschutzmanagement des Unternehmens geprüft. Datenschutzrechtlich relevante Prozesse des Unternehmens werden in einem sog. internen Verfahrensverzeichnis erfasst. Dieses Verfahrensverzeichnis beinhaltet die vom Unternehmen an xDSB Datenschutz gemeldeten Unternehmensprozesse, bei welchen personenbezogene Daten verarbeitet werden. Das Verfahrensverzeichnis enthält unter anderem Angaben zu den verarbeiteten personenbezogenen Daten, den mit der Verarbeitung verfolgten Zwecken, die Zugriffsberechtigungen, die Weitergabe dieser Daten als auch die Löschung der Daten. Die Vereinbarung dieser im Verfahrensverzeichnis erfassten Datenverarbeitungen werden auf Vereinbarkeit mit deutschem Datenschutzrecht geprüft und bewertet. Hierbei werden auch die gem. § 9 BDSG (und Anlage) bestehenden Anforderungen an die technische und organisatorische Umsetzung des Datenschutzes überprüft. Das Unternehmen muss darüber hinaus eine entsprechend erforderliche Überprüfung regelmäßig durchführen.

Die Prüfung muss zu dem Ergebnis kommen, dass keine oder nur marginale Beanstandungen hinsichtlich der Einhaltung der deutschen und europäischen Datenschutzregelungen zu verzeichnen sind.

Die Prüfung des Datenschutzmanagements eines Unternehmens erfolgt im Jahr der Erstvergabe durch eine Komplettprüfung, in den Folgejahren durch Prüfung von Veränderungen und der Überprüfung per Stichproben/ Audits.

Bei der Durchführung von Stichproben/Audits werden anhand von Checklisten bestimmte datenschutzrechtlich relevante Bereiche des Unternehmens bzw. im Verfahrensverzeichnis dokumentierte Verfahren überprüft und beurteilt. Ein Teilbereich des Audits/Stichproben muss den technischen Datenschutz betreffen (etwa technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage).

xDSB Datenschutz nimmt die Prüfung im Rahmen der Stellung als nach BDSG unabhängigem Datenschutzbeauftragten des Unternehmens wahr. Es wird versichert, dass xDSB Datenschutz hierbei unabhängig und weisungsfrei in Wahrnehmung der Funktion des betrieblichen Datenschutzbeauftragten gem. § 4f Abs. 2 und Abs. 3 BDSG auftritt und prüft und keine Interessenskollision gemäß den Anforderungen an betriebliche Datenschutzbeauftragte besteht.

Gültigkeitsdauer des Gütesiegels

Das Gütesiegel wird für jeweils ein Kalenderjahr vergeben.
Die Neuvergabe für das Folgejahr bedarf einer erneuten, jedoch vereinfachten Prüfung der genannten Prüfpunkte.

Voraussetzung für die Vergabe des Gütesiegels

xDSB Datenschutz muss der betriebliche Datenschutzbeauftragte des Unternehmens sein, welcher gem. § 4f Abs. 2 und Abs. 3 BDSG unabhängig und weisungsfrei auftritt.
Das interne Verfahrensverzeichnis und die technischen und organisatorischen Maßnahmen (§ 9 BDSG und Anlage) des Unternehmens wurden von xDSB Datenschutz erstellt, geprüft und mittels Checklisten bewertet.

Bewertungen der erfassten Verfahren:

OK (grün)	(gesetzliche Datenschutzvorschriften vollumfänglich erfüllt)
bedingt OK (gelb)	(leichte Defizite im Datenschutz mit Verbesserungspotential)
nicht OK (rot)	(schwerwiegender Verstoß gegen Datenschutzvorschriften).

Vergabekriterien des Gütesiegels

- Es existiert ein aktuelles und vollständiges öffentliches und internes Verfahrensverzeichnis.
- Die Prüfung des internen Verfahrensverzeichnis ergibt keine Bewertung „nicht OK“
- max. 15% der geprüften Verfahren des internen Verfahrensverzeichnisses sind „bedingt OK“, alle anderen geprüften Verfahren sind OK .
- ein Datenschutzbeauftragter ist bestellt und er erfüllt die hohen Anforderungen nach dem Beschluss des Düsseldorfer Kreises vom 24./25. November 2010 (Fachkunde und Unabhängigkeit).
- Alle Mitarbeiter, die mit personenbezogenen Daten in Kontakt geraten können, sind zum Thema betrieblicher Datenschutz geschult.
- Alle Mitarbeiter, die mit personenbezogenen Daten in Kontakt geraten können, sind gem. § 5 BDSG auf das Datengeheimnis verpflichtet.
- Auftragsdatenverarbeitungen sind schriftlich geregelt und die vom Gesetzgeber geforderte schriftliche Vereinbarung wurde auf Vereinbarung mit § 11 BDSG geprüft.

Ablauf und Dokumentation

xDSB Datenschutz dokumentiert die Verfahrensverzeichnisse in ihrer Experten-Software. Bei Durchführung eines Audits werden im Vorfeld der Prüfung schriftlich die Bereiche benannt, welche auditiert werden. Bei der Durchführung von Stichproben werden vorher keine Ankündigungen gemacht.

Die Prüfung wird schriftlich dokumentiert und für den Zeitraum der Gültigkeit des Gütesiegels archiviert.

Nach Abschluss der Prüfung wird das Resultat dem Unternehmen bekannt gegeben. Das Unternehmen kann anschließend einmalig Einwände vorbringen, welche von xDSB Datenschutz überprüft werden.

xDSB Datenschutz prüft abschließend, ob die Vergabekriterien für das Gütesiegel erfüllt wurden und gibt dem Unternehmen seine Entscheidung bekannt.

Verleihung des Gütesiegels und Ablehnung

Stellt xDSB Datenschutz fest, dass die Vergabekriterien erfüllt wurden, wird dem Unternehmen das Datenschutz-Gütesiegel verliehen.

Stellt xDSB Datenschutz fest, dass die Vergabekriterien nicht erfüllt wurden, wird das Datenschutz-Gütesiegel nicht verliehen. Dem Unternehmen steht es jedoch frei, binnen acht Wochen vorhandene Mängel zu beseitigen und die Beseitigung nachzuweisen. xDSB Datenschutz wird anschließend erneut über eine Vergabe des Gütesiegels endgültig entscheiden. Wird von xDSB Datenschutz die Verleihung für das laufende Kalenderjahr endgültig abgelehnt, hat das Unternehmen für das laufende Kalenderjahr kein Anrecht auf das Gütesiegel; über die Vergabe des Gütesiegels kann dann erst wieder im Folgejahr entschieden werden.

Erneuerung des Gütesiegels

Das Gütesiegel kann im Folgejahr erneut mit Gültigkeit für das Folgejahr vergeben werden. Hierzu werden Veränderungen im Vergleich zum Vorjahr (z.B. durch Einsicht in das interne Verfahrensverzeichnis) beurteilt. Darüber hinaus muss ein Audit/Stichproben durchgeführt werden.
Bei der Durchführung von Stichproben/Audits werden anhand von Checklisten bestimmte datenschutzrechtlich relevante Bereiche des Unternehmens bzw. dokumentierte Verfahren überprüft und beurteilt. Hierbei sind mindestens 15% der im internen Verfahrensverzeichnis dokumentierten Verfahren durch Stichproben zu überprüfen. Ein Teilbereich des Audits/Stichproben muss den technischen Datenschutz betreffen (etwa technische und organisatorische Maßnahmen nach § 9 BDSG).

Für die Erneuerung des Gütesiegels gelten folgende Vergabekriterien:

- Die Voraussetzung für die Vergabe des Gütesiegels bestehen fort
- Die Stichproben/Audit ergeben keine Bewertungen „nicht OK“
- max. 15% der in den Stichproben/Audit geprüften Verfahren sind „bedingt OK“, alle anderen geprüften Verfahren sind OK .
- ein Datenschutzbeauftragter ist bestellt und er erfüllt die hohen Anforderungen nach dem Beschluss des Düsseldorfer Kreises vom 24./25. November 2010 (Fachkunde und Unabhängigkeit).
- Alle Mitarbeiter, die mit personenbezogenen Daten in Kontakt geraten können, sind zum Thema betrieblicher Datenschutz geschult.
- Alle Mitarbeiter, die mit personenbezogenen Daten in Kontakt geraten können, sind gem. § 5 BDSG auf das Datengeheimnis verpflichtet.
- Es existiert ein aktuelles und vollständiges öffentliches und internes Verfahrensverzeichnis.

- Auftragsdatenverarbeitungen sind schriftlich geregelt und der vom Gesetzgeber geforderte Vertrag wurde auf Vereinbarung mit § 11 BDSG geprüft.

Im Übrigen gelten die o.g. Regeln zur Verleihung des Gütesiegels und Ablehnung entsprechend.

Nutzungsrechte an dem Gütesiegel

Alle Rechte am Gütesiegel liegen bei xDSB Datenschutz. Das Gütesiegel ist urheberrechtlich geschützt. Alleine xDSB Datenschutz ist berechtigt, das Gütesiegel zu verleihen und hieran Nutzungsrechte einzuräumen.

Mit der Vergabe des Gütesiegels durch xDSB Datenschutz wird dem geprüften Unternehmen das einfache (nicht-ausschließliche) Nutzungsrecht eingeräumt, das von xDSB Datenschutz überlassene Gütesiegel zu nutzen, zu vervielfältigen und öffentlich wiederzugeben oder zugänglich zu machen.

Eine Wiedergabe kann beispielsweise über eine Darstellung in Printmedien, im Internet oder in E-Mails erfolgen.

Vertraulichkeit

xDSB Datenschutz führt die Prüfung zur Vergabe des Gütesiegels unter Wahrung der Vertraulichkeit und von Geschäfts- und Betriebsgeheimnissen durch. Die Verschwiegenheitspflichten gem. § 4f Abs. 4 BDSG werden gewahrt.

Karlsruhe, 06.08.2016

Michael Bätzler, EDV-Sachverständiger, TÜV-Datenschutzauditor, Ext. Datenschutzbeauftragter (IHK)
RA Thomas Steinle, LL.M., Fachanwalt für Informationstechnologierecht, Ext. Datenschutzbeauftragter (IHK)