Prüfschema

Erteilung des Datenschutz-Siegels „Datenschutzkonform“

durch die Prüfstelle

greeneagle certification GmbH
Frankenstraße 18a
20097 Hamburg

Dokumententitel: Erteilung des Datenschutz-Siegels „Datenschutzkonform“
Dokumentenversion: 1.0
Datum: 10.05.2015
Status: veröffentlicht

greeneagle certification GmbH

Frankenstraße 18a, 20097 Hamburg
+49 40 790235 - 200
+49 40 790235 - 220

Inhaltsverzeichnis

1 Vorwort

Zum Nachweis der Einhaltung und der erfolgreichen Umsetzung der Anforderung von Datenschutz und Datensicherheit bietet die green**eagle** certification GmbH ein eigenes Datenschutz-Siegel an.

Dieses Siegel soll privaten und öffentlichen Unternehmen die Möglichkeit geben, Ihre Bemühungen im Bereich Datenschutz und Datensicherheit sowie die erfolgreiche Umsetzung datenschutzrechtlicher Vorgaben zu dokumentieren.
Dabei ist eine Zertifizierung von Unternehmensprozessen, Unternehmensteilen, einzelner Verfahren, IT-Produkte oder IT-basierter Dienstleistungen möglich. Bei Bestätigung der Konformität mit den geltenden datenschutzrechtlichen Vorgaben und der Einhaltung dieser soll das Prüfsiegel

„DATENSCHUTZKONFORM“

erteilt werden.

Das Siegel wird von der beim ULD anerkannten Prüfstelle für Recht und Technik, der green**eagle** certification GmbH, nach den hier dokumentierten Regeln erteilt:

2 Prüfungsgrundlage

Die Prüfung erfolgt auf Grundlage des jeweils einschlägigen Datenschutzrechts (BDSG oder landesrechtliche Regelungen), TKG und TMG sowie weiterer datenschutzrechtlicher gesetzlicher Vorgaben sowie der Grundlage von etablierten Standards zum Informationssicherheitsmanagement (ISO 27001 und BSI 100-x).

Die Umsetzung der Informationssicherheitsmaßnahmen nach ISO27001 auf der Basis von IT-Grundschutz des BSI ist als probates Mittel zur Umsetzung der nach § 9 BDSG geforderten technischen und organisatorischen Maßnahmen anerkannt. Bestimmte und im Einzelfall angemessene Inhalte des IT-Grundschutzkatalogs fließen dabei in das Prüfverfahren ein.

3 Prüfprozess

Die Bestätigung der Einhaltung datenschutzrechtlicher Vorgaben erfolgt durch die Erteilung eines Siegels des Auftragnehmers. Das Siegel wird für 2 Jahre erteilt. Die Prüfung erfolgt anhand der Anforderungen des BDSG, der Informationssicherheitsstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie weiterer bereichsspezifischer datenschutzrechtlicher Vorgaben.
Der Prüfprozess wird dabei nach dem folgenden Prüfschema durchgeführt.

3.1 Initialaudit (Erst-Erteilung des Prüfsiegels)

Das Audit verläuft als Vollaudit in folgenden Etappen:

Etappe	Inhalt	Ausführungsort
1	OPTIONAL Voraudit	Antragsteller
2	Phase 1 - Prüfung der Dokumente	Prüfstelle
3	Phase 2 – Umsetzungsprüfung Vor Ort (Stichprobenprüfung)	Antragsteller
4	Erstellen des Prüfbericht	Prüfstelle
5	Auditabschluss, Erteilung des Prüfsiegels	Prüfstelle

Tabelle 1: Phasen des Initialaudits

3.1.1 Voraudit (optional)

Zur Absicherung eines reibungslosen Verlaufs des Hauptaudits wird empfohlen, ein Voraudit durchzuführen. Ziel des Voraudits ist es, die bestehenden Dokumente zu sichten, erste Gespräche über den Umsetzungsstand des Datenschutzes sowie der Datensicherheit zu führen sowie stichpunktartig Implementierungen zu prüfen.
Sinn des Voraudits ist die Überprüfung, ob ein Audit prinzipiell zu einem positiven Ergebnis führen kann. Das Voraudit dient nicht dem Zweck, den Antragsteller zu beraten oder auf später zu prüfende Aspekte vorzubereiten. Das Ergebnis des Voraudits wird im Prüfbericht des Hauptaudits kurz dokumentiert.
Werden im Voraudit bereits Prüfaspekte positiv geprüft, kann eine erneute Prüfung bei gleichen Rahmenbedingungen im Hauptaudit entfallen. Positive Prüfergebnisse werden in diesem Fall in den Hauptauditbericht übernommen.

3.1.2 Phase 1: Prüfung der Dokumente

Für die Überprüfung müssen dem Auditteam zum Auditbeginn mindestens nachfolgend genannte Dokumente als Grundlagendokumentation übergeben werden (in elektronischer Form):

- Benutzerhandbuch/Produktdokumentation für den Untersuchungsgegenstand,
- Datenschutzerklärung,

- interne Richtlinien zum Datenschutz und zur Datensicherheit,
- Verfahrensverzeichnisse
- Verträge zur Auftragsdatenverarbeitung inklusive der technischen und organisatorischen Maßnahmen; zum einen solche, in denen der Antragsteller als Auftragnehmer iSd § 11 BDSG auftritt, zum anderen solche, in denen er als Auftraggeber i.S.d. § 11 BDSG auftritt,
- IT-Sicherheitskonzept, Zertifizierungen (z.B. nach ISO/IEC 27001, ISAE 3402 o.a.),
- etwaige Hosting-Verträge, Verträge über IT-Dienstleistungen.

Die Dokumente werden durch das Auditteam bewertet. Die Prüfergebnisse werden im Prüfbericht dokumentiert. Gegebenenfalls festgestellte Abweichungen und Empfehlungen werden dem Auftraggeber zeitnah mitgeteilt und Fristen zur Nachbesserung festgelegt.

Abschließender Bestandteil der Phase 1 ist die Vorbereitung der Vor-Ort-Prüfung (Phase 2) mit folgenden Schritten:

- Wurden schwerwiegende Abweichungen festgestellt, so sind diese durch den Antragsteller grundsätzlich vor der Weiterführung des Audits zu beseitigen. Dies ist durch das Auditteam zu prüfen.
- Der Auditteamleiter bespricht zusammen mit dem Antragsteller, welche Komponenten vor Ort überprüft werden sollen.
- Stellt der Auditteamleiter fest, dass spezifische Fachkenntnisse zur Prüfung einzelner Komponenten im Informationsverbund fehlen, ist das Auditteam durch entsprechende Auditoren oder Fachspezialisten zu erweitern.

3.1.3 Phase 2: Umsetzungsprüfung vor Ort (Stichprobenprüfung)

Nach der Prüfung der Dokumente erfolgt die Überprüfung der Übereinstimmung der Dokumente mit der Praxis. Diese Überprüfung erfolgt in Form von Interviews, Ortsbegehungen sowie ggfs. Konfigurationsprüfungen am System. Dabei können die Dokumentenprüfung und die Vor-Ort-Prüfung auch parallel durchgeführt werden.

Der Antragsteller gewährleistet für die Vor-Ort-Prüfung die Teilnahme kompetenter Interviewpartner. Gegebenenfalls festgestellte Abweichungen und Empfehlungen werden dem Auftraggeber unverzüglich mitgeteilt und Fristen zur Nachbesserung festgelegt. Alle Abweichungen sind bis spätestens zur Fertigstellung des Prüfberichtes zu beheben bzw. auszugleichen.

3.1.4 Prüfbericht

Das Auditteam fasst die Ergebnisse des Audits in einem Prüfbericht zusammen und gibt ein Gesamtvotum ab (zum Aufbau und der Darstellung des Berichtes vgl. Punkt 4.1).

Sollten während der Prüfungen im Rahmen des Audits Schwachstellen erkannt bzw. Nachforderungen erhoben werden, besteht die Möglichkeit von Nachbesserungen durch den Antragsteller bis zum Abschluss des Prüfberichtes. Nach einer Nachprüfung durch das Auditteam fließen die nachgebesserten Details in den finalen Prüfbericht mit ein.

3.1.5 Auditabschluss, Erteilung des Prüfsiegels

Das Audit wird mit einem finalen Prüfbericht sowie bei positiver Bewertung der Audit-Ergebnisse mit einem Siegel der Prüfstelle erteilt.

3.2 Wiederholungsaudit (nach zwei Jahren)

Das nach jedem Hauptaudit (Initialaudit oder Wiederholungsaudit) erteilte Siegel wird für 2 Jahre verliehen. Nach dieser Zeit ist für eine erneute Erteilung des Zertifikates ein Wiederholungsaudit durchzuführen. Gleiches gilt grundsätzlich bei wesentlichen Veränderungen am Untersuchungsgegenstand.

4 Ergebnisdokumentation

4.1 Der Prüfbericht

Der Prüfbericht teilt sich in folgende 4 Teile auf:

- Allgemeiner Teil: Dokumentation allgemeiner Informationen, wie etwa zur überprüften Institution, dem Auditteam, dem Untersuchungsgegenstand sowie einer Zusammenfassung.
- Datenschutzrechtliche Bewertung: Dokumentation der Ergebnisse der Prüfung der datenschutzrechtlichen Zulässigkeit hinsichtlich der Datenverwendung sowie der datenschutzrechtlichen Grundsätze und Pflichten.
- Technische und organisatorische Maßnahmen: Dokumentation der Ergebnisse der Prüfung der umgesetzten technischen und organisatorischen Maßnahmen.
- Gewährleistung der Betroffenenrechte: Dokumentation der Ergebnisse der Prüfung der Gewährleistung und Umsetzung der Betroffenenrechte.

Die verschiedenen Teile können je nach Untersuchungsgegenstand unterschiedlich stark ausgeprägt sein.
Der Auditbericht wird in deutscher Sprache verfasst und in digitaler Form übergeben.

4.2 Prüfmethodik

Die Prüfung beinhaltet folgende methodischen Bestandteile:

- Dokumentationsprüfung
- Interviews und Befragungen
- Inaugenscheinnahme z. B. Begehung, Einsicht in Konfigurationen usw.
- Durchsicht von Unterlagen, z. B Richtlinien, Anweisungen usw.
- Analyse und ggf. Verwertung von Unterlagen Dritter, z. B. Protokolle oder Verträge
- Beobachtung von Aktivitäten und Arbeitsabläufen

4.3 Bewertungsmaßstäbe und Auswirkungen

Die getroffenen Maßnahmen zur Umsetzung der Anforderungen an Datenschutz und Datensicherheit können unterschiedlich bewertet werden, wobei grundsätzlich folgende Bewertungen vorgenommen werden:

Erfüllungsgrad	**Erläuterung**	**Auswirkungen**
Umgesetzt	Die getroffene Maßnahme erfüllt vollständig die Anforderungen an Datenschutz und Datensicherheit	Siegel wird erteilt
Empfehlung	Bei umgesetzten Maßnahmen können gegebenenfalls Hinweise zur weiteren Erhöhung von Datenschutz und Sicherheit	Siegel wird erteilt

Erfüllungsgrad	Erläuterung	Auswirkungen
	gegeben werden.	
Geringfügige Abweichung	Einzelne getroffene Maßnahmen sind nicht vollständig oder unzureichend umgesetzt. Dabei können ggfs. fehlende technische Maßnahmen durch organisatorische ausgeglichen werden oder umgekehrt. Bei nicht ausreichendem Ausgleich kann hieraus eine geringfügige Abweichung erfolgen.	Siegelerteilung ist Abhängig von den getroffenen ausgleichenden Maßnahmen sowie von der Anzahl der festgestellten geringfügigen Abweichungen
Schwerwiegende Abweichung	Wesentliche Maßnahmen sind nicht oder unzureichend umgesetzt.	Wurden schwerwiegende Abweichungen festgestellt, so sind diese durch den Antragsteller grundsätzlich vor der Weiterführung des Audits zu beseitigen. Nicht behobene schwerwiegende Abweichungen können zum Abbruch des Audits führen.

Tabelle 2: Bewertungsmaßstäbe

5 Auditoren

Der eingesetzte Auditteamleiter ist ein beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zugelassener Mitarbeiter für die Bereiche Recht und Technik.

Zur Absicherung spezifischer Fachkenntnisse können durch den Auditteamleiter bei Bedarf weitere Co-Auditoren oder Fachexperten einbezogen werden.