Hinweise für ips-Auditoren / ips-Prüfstellen

1. Hinweise zur Auditierung nach ips

Die Auditierung (auch Begutachtung) eines Webportals nach ips richtet sich an dem jeweils aktuellen ips-Kriterienkatalog mit seinen Modulen aus. Wie die Module anzuwenden sind und was zu prüfen ist, kann den im Kriterienkatalog veröffentlichten allgemeinen Hinweisen entnommen werden.

Für eine erfolgreiche Vergabe des ips-Siegels ist es notwendig, dass der datenschutz cert GmbH ein aussagekräftiges Hauptgutachten (auch Audit-Report) sowie ein Kurzgutachten vorgelegt werden. Die nachfolgenden Hinweise sollen deren Erstellung unterstützen.

Die datenschutz cert GmbH ist für Anregungen, Wünsche und Kritik immer dankbar.

Bremen, den 16. April 2018

Irene Karper

ppa. Dr. Irene Karper LL.M. Eur.
datenschutz cert GmbH

2. Hauptgutachten / Audit-Report

Die Form und Methodik der Begutachtung ist dem ips-Auditor bzw. der ips-Prüfstelle grundsätzlich freigestellt. Bei der Erstellung des Hauptgutachtens sollte allerdings darauf geachtet werden, dass der Prüfgegenstand, die angewandten Prüfkriterien und die Ableitung der Ergebnisse nachvollziehbar dokumentiert sind.

Das Hauptgutachten zur Auditierung eines Webportals gemäß ips sollte sich daher am Aufbau des ips-Kriterienkataloges orientieren und insbesondere die gleiche Reihenfolge der in den anwendbaren ips-Modulen aufgeführten Prüfkriterien wiedergeben.

Ein ips-Hauptgutachten bzw. ein Auditreport zur Vorlage bei der datenschutz cert GmbH muss inhaltlich zudem mindestens zu folgenden Aspekten Stellung beziehen:

- Organisatorische und formale Angaben zum Audit
  - das mit der Auditierung angestrebte Gütesiegel ips (z.B. „Audit-Report des Webportals www.xy.de nach ips“)
  - Untersuchte Organisation, Name, Anschrift, URL

  - genaue Bezeichnung des Untersuchungsgegenstands, Abgrenzung zu den nicht auditierten Bereichen
  - Auditoren (Recht/Technik), Name, Anschrift
  - Zeitraum der Auditierung
- Angewandte Methodik
  - z.B. Prüfung von Dokumenten des Auftraggebers, Führung von Mitarbeitergesprächen, Durchführung von Stichproben vor Ort (Site Visit), Penetrationstests der Webserver, Plausibilitätstests durch Besichtigung der Webseiten.
- Grundlagen der Auditierung, z.B.:
  - Ggf. eingesehene Dokumente, Zertifikate, Prüfdokumentationen
  - Ggf. befragte Abteilungen/Arbeitsbereiche/Unternehmensorgane
  - Ggf. Gegenstand der Stichproben (Testaccounts, Test-Bestellungen etc.)
  - Ggf. Ortsbesichtigung, Standort, Adresse, Dauer, Teilnehmer
- Erklärung der Auditoren, z.B.:
  - „Ich bestätige, dass ich das Audit im Einklang mit den relevanten Regelwerken und Normen, den Regelungen des Auditorenvertrages sowie den Vergabe- und Nutzungsbedingungen der datenschutz cert GmbH durchgeführt habe und damit insbesondere den Untersuchungsgegenstand des Antragstellers objektiv, neutral, weisungsfrei, unabhängig und korrekt auditiert habe. Ich habe keinerlei Verbindung zum Untersuchungsgegenstand des Antragstellers. Ich war in den letzten zwei Jahren vor Beginn dieses Verfahrens nicht für den Untersuchungsgegenstand des Antragstellers beratend tätig.“ Ort, Datum, Unterschrift;
- Kurzdarstellung des Untersuchungsgegenstands
- Zusammenstellung des für den konkreten Auditgegenstand anwendbaren Prüfkriterien/Anforderungen
  - Differenziert nach ips-Modulen und dessen Gewichtung.
- Vorgefundene Umstände pro Prüfkriterium
- Bewertung der vorgefundenen Umstände pro Prüfkriterium
- Votum des Auditors
  - Zusammenfassung der Auditergebnisse / Management Summary
  - Vorschlag an die datenschutz cert GmbH.

3. Kurzgutachten

ips-Auditoren bzw. ips-Prüfstellen legen der datenschutz cert GmbH neben dem Hauptgutachten auch einen *Entwurf* eines Kurzgutachtens vor, welches von der datenschutz cert GmbH *ergänzt* und auf den Webseiten veröffentlicht wird. Das auf der Grundlage des Hauptgutachtens zu erstellende Kurzgutachten soll dazu dienen, dem Nutzer des Web-Angebotes mit einem kurzen Überblick die Schwerpunkte des Hauptgutachtens zu erläutern. Neben den formalen Angaben (Prüfungszeitpunkt, Auditor/Prüfstelle, Anbieter, URL) soll das Kurzgutachten Aufschluss über die zur Prüfung herangezogenen ips-Module bieten sowie die wesentlichen Ergebnisse aufführen. Im Anschluss daran enthält das Kurzgutachten schließlich Hinweise auf besonders datenschutzfreundliche Umstände und Funktionen des Angebotes.

Das Kurzgutachten wird über das ips-Logo verlinkt zum Server der datenschutz cert GmbH, so dass Nutzer beim Klick auf das Logo unmittelbar das Kurzgutachten lesen können.

Nachfolgend werden die wesentlichen Inhalte des Kurzgutachtens erörtert.

3.1. Allgemeines zu ips

Hier ist kurz anzugeben, was eine Vergabe des Siegels gemäß ips beinhaltet, z.B.:

Die XY GmbH hat das Web-Angebot unter www.XY.de nach den internet privacy standards (ips) prüfen lassen. Damit hat sie sich höchsten Anforderungen unterworfen, die zum einen die Einhaltung datenschutz- und verbraucherschutzrechtlicher Vorschriften sicherstellen als auch die Sicherheitsvorkehrungen nach dem aktuellen Stand der Technik beinhalten. Der ips-Kriterienkatalog ist abrufbar unter www.datenschutz-cert.de .

Die internet privacy standards werden als bundesweit gültiges Gütesiegel für Webportale von der Initiative D21 der Bundesregierung empfohlen und sind mit zahlreichen Datenschutzbeauftragten der Länder und des Bundes abgestimmt. Eine Vergabe von ips entspricht einem hohen Prüfungsmaßstab. Sie sehen also: Bei dem Anbieter sind Sie datenschutzrechtlich "gut aufgehoben".

3.2. Anbieter und URL des Angebotes

Hier ist die vollständige URL des geprüften Angebotes sowie der Anbieter mit Name der juristischen Person und mindestens der Postanschrift zu benennen.

3.3. Angaben zum ips-Auditor/zur ips-Prüfstelle

Bei juristischen Personen erfolgen hier die Unternehmensangaben mit Nennung des verantwortlichen Prüfstellenleiters, im Übrigen die Nennung des Auditors, des evtl. eingesetzten Hilfspersonal und Kontaktangaben.

3.4. datenschutz cert GmbH

Sodann sind die datenschutz cert GmbH und die von ihr vergebene Nummer zu benennen:

datenschutz cert GmbH
(Ansprechpartner)
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0471 – 696632-50
Fax.: 0471-696632-51
E-Mail: office@datenschutz-cert.de

Bei erfolgreicher Vergabe des ips-Siegels wird durch die datenschutz cert GmbH eine individuelle Nummer vergeben und in das Kurzgutachten eingetragen.

Dieses ips-Gütesiegel wird erteilt unter der Nummer DSC.XXX.XXXXXX.

Die Nummer kann bei der datenschutz cert GmbH mit Abschluss des Verfahrens erfragt werden und befindet sich auch in der unter www.datenschutz-cert.de abrufbaren Liste.

3.5. Umfang der Prüfung nach ips

Der Auditor soll an dieser Stelle erläutern, ob es sich um eine Erst-Auditierung oder um eine Auditierung mit dem Ziel der erneuten Vergabe des ips-Siegels handelt, welche Version des ips-Kriterienkataloges und welche ips-Module zur Prüfung herangezogen wurden und welche prozentuale Gewichtung den jeweiligen Modulen zugerechnet wurden.

Beispiel: Das Webangebot wurde im Juli 2018 auf der Grundlage des ips-Kriterienkatalogs in der Version XX geprüft. Die erstmalige Prüfung erfolgte im August 2011. Die Begutachtung nach ips umfasst nicht nur die Überprüfung der für jeden Nutzer sichtbaren Bereiche wie Datenschutzerklärung, Impressum, IP-Adresse, Cookies u.V.m. anhand der einschlägigen gesetzlichen Vorgaben, sondern durchleuchtet auch die Netzwerksicherheit des Anbieters und die interne Organisation der Datenverarbeitung (sog. Datenschutzmanagement). So können Sie als Nutzer sicher sein, dass Technik und Mitarbeiter des Anbieters Ihre Rechte wirklich ernst nehmen - und damit Ihr Persönlichkeitsrecht schützen.

Über das Portal werden in unterschiedlicher Intensität personenbezogene Daten erfasst. So sind im Rahmen des Informations-Angebots Transparenz und Datensparsamkeit zu beachten. Im Rahmen der Individual-Dienstleistung ist insbesondere der Bereich der Online-Anmeldung relevant. Den zu übermittelnden

Daten kommt eine hohe Schutzbedürftigkeit zu. Ferner gelten aufgrund der Sensibilität der Kundendaten höchste Anforderungen für die technisch-organisatorische Sicherheit im Rahmen des Datenschutzmanagements. Aufgrund der unterschiedlichen Schutzbedürftigkeit wurde folgende Gewichtung zugrunde gelegt:

- Informations-Angebot: 20%
- Individuelle Dienstleistung: 30%
- Datenschutzmanagement: 50%

3.6. Zusammenfassung der Prüfergebnisse

An dieser Stelle werden die Ergebnisse der Auditierung dargestellt. Hier bietet sich vor allem die Gelegenheit, Besonderheiten des Angebotes im Hinblick auf datenschutzfreundliche bzw. datensparsame Implementierungen hervorzuheben.

Beispiel: Das Angebot zeichnet sich durch folgende Rahmenbedingungen aus:

- vorbildliche Transparenz der Datenverarbeitung für den Nutzer
- Verwendung hoher Sicherheitsstandards bei der Übermittlung personenbezogener Daten.

Der Anbieter setzt in allen Bereichen die gesetzlichen Anforderungen um.

Die vom Anbieter getroffenen technisch-organisatorischen Sicherheitsmaßnahmen gehen größtenteils vorbildlich über das Maß hinaus und gewähren die Sicherheit der Daten nach dem aktuellen Stand der Technik. Der Benutzer wird einfach verständlich über die Funktion des Webportals sowie über Datenerhebung und -nutzung aufgeklärt.

Der Anbieter setzt in den geprüften Onlinebereichen die Anforderungen des Kriterienkatalogs ips um und erhält daher das Online-Gütesiegel.

4. Form und Vorlage bei der datenschutz cert GmbH

Das Kurzgutachten kann gemeinsam mit dem Hauptgutachten (Audit-Report) bei der datenschutz cert GmbH eingereicht werden. Die Kontaktdaten lauten:

datenschutz cert GmbH
Prüfstelle ips
Konsul-Smidt-Str. 88a
28217 Bremen
Fax.: 0471-696632-51
E-Mail: office@datenschutz-cert.de

Alle Dokumente können vorzugsweise elektronisch eingereicht werden. Das Kurzgutachten sollte möglichst im Format „Textdatei“ bei der datenschutz cert GmbH eingereicht werden. Für eine verschlüsselte Datenübertragung können Sie unseren pgp-Schlüssel nutzen.