Die internet privacy standards (Vers. 3.5) – Einführung und allgemeine Hinweise zur Anwendung

datenschutz cert GmbH
29. Juli 2020

datenschutz cert

Inhaltsverzeichnis

1. 1. Vorwort zur Neuauflage (Version 3.5)

Das Gütesiegel ips – internet privacy standards – ist ein bundesweit seit 2001 etabliertes Siegel für Webportale und Webservices. Es wird u.a. vom Bundesjustizministerium, Verbraucherschutzverbänden und der Initiative D21 der Bundesregierung empfohlen. Die Vergabe für das ips Gütesiegel wird nach einem Audit durch lizenzierte ips-Auditoren von der unabhängigen Vergabestelle der datenschutz cert GmbH durchgeführt.

Die für Webangebote geltenden datenschutz-, verbraucherschutzrechtlichen und sicherheits-technischen Anforderungen unterliegen einer ständigen Entwicklung. Der ips-Kriterienkatalog wird daher fortlaufend von der Vergabestelle aktualisiert. Die Prüfung eines Webportals oder Webservices mit ips anhand der ständig optimierten Prüfkriterien verdeutlicht die hohe Qualität eines Webangebotes.

Mit der nun erfolgten Neuauflage 3.5 wurden zudem die Neuerungen der Anlage 31b zum Bundesmantelvertrag-Ärzte der „Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Absatz 4 SGB V vom 21. Oktober 2016 in der Fassung vom 31. Mai 2020“ hinsichtlich der Prüfung von Online-Videosprechstunden einbezogen. Bereits im Mai 2018 wurden die Kriterien u.a. an Gesetzesänderungen zum Datenschutz- und Fernabsatzrecht, die aktuelle Rechtsprechung und die Auslegung der Datenschutz-Aufsichtsbehörden (z.B. zum Thema Cookies) angepasst. Dabei wurde die Anzahl der Module reduziert und komprimiert. Vor allem aber wurden die Anforderungen der EU-Datenschutzgrundverordnung (DSGVO) an Webportale und Webservices aufgenommen. Damit unterstützt eine Prüfung und das Gütesiegel anhand der ips-Kriterien die in Art. 5 DSGVO vorgegebenen Rechenschaftspflicht der Betreiber.

Zum Redaktionsschluss waren die Entwürfe des Europäischen Rates und des Europäischen Parlaments und der Europäischen Kommission für eine E-Privacy-Verordnung noch nicht durch den sogenannten Trilog abschließend konsolidiert. Die in den letzten Entwürfen vorgesehenen Aspekte finden daher in dieser Fassung des ips-Kriterienkataloge größtenteils noch keine Berücksichtigung.

Die Autoren sind für Anregungen, Wünsche und Kritik immer dankbar.

Bremen, im Juli 2020

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

Alisha Gühr
datenschutz cert GmbH

2. Zielsetzung

Die internet privacy standards bilden einen Katalog von Qualitätskriterien, der als Grundlage für die Auditierung von Online-Dienstleistungen angewandt wird. Die Qualitätskriterien decken eine Prüfung anhand datenschutzrechtlicher, verbraucherschutzrechtlicher sowie datensicherheits-technischer Anforderungen ab. Mit der Vergabe von ips soll nachgewiesen werden, dass das Webportal bzw. der geprüfte Webservice zum Auditzeitpunkt den rechtlichen Anforderungen entsprechen. Die Prüfung erfolgt dabei durch lizenzierte ips-Auditoren, die in den genannten Bereichen nachgewiesen fachkundlich und unabhängig tätig sind. Geprüfte und mit ips ausgezeichnete Anbieter können so ihrer Rechenschaftspflicht nach Art. 5 DSGVO nachkommen. Zugleich soll das Siegel ips den Benutzern des Webportals / Webservices signalisieren, dass es sich um einen vertrauenswürdigen Anbieter handelt, der die Einhaltung des Daten- und Verbraucherschutzes ernst nimmt.

Mit dem Kriterienkatalog werden

- die gesetzgeberische Intention für ein Datenschutzaudit und für Datenschutz-Gütesiegel gezielt und praxisnah umgesetzt,
- die Datenschutzfolgeabschätzung bzgl. der Online-Datenverarbeitung über das Webportal / den Webservice unterstützt,
- Anreize für besonders datenschutzfreundliche Lösungen (privacy by design) geschaffen,
- unterschiedlichste Online-Dienstleistungen bewertet und
- die speziellen Anforderungen der jeweiligen Online-Funktionen berücksichtigt.

3. Die Module

Den internet privacy standards liegt der Gedanke zugrunde, dass sämtliche Online-Dienstleistungen in Teilbereiche, sog. Module, aufgespalten und durch Zusammenstellung des jeweils „passenden" Kriterienwerkes abgebildet werden können. Mit dem aktuellen ips Kriterienkatalog gibt es fünf Module, mit denen die Prüfung von Online-Shops über Online-Videosprechstunden, Online-Serviceportalen bis hin zum reinen Informationsportal für Kunden möglich ist. Der im konkreten Verfahren eingesetzte ips-Auditor ist dabei aufgefordert, die jeweils anwendbaren Module auszuwählen.

3.1. Die Module im Überblick

M 1 Info-Abruf

Das Modul „Info-Abruf" umfasst Bereiche, die ohne weitere Dateneingabe durch Aufruf der Homepage und Unterseiten abrufbar sind und im Wesentlichen Informationen enthalten. Hier werden insbesondere Aspekte der Transparenz (z.B. Anbieterkennzeichnung, Datenschutzerklärung) sowie der Umgang mit Nutzerdaten (IP-Adresse, Cookies, Social Plugins usw.) geprüft.

M 2 Individual-Dienstleistung

Der Bereich Individual-Dienstleistung erfasst den eigentlichen Kern der Online-Dienstleistung, also die vom Nutzer abrufbaren Online-Services und Webformulare. Unter

diesem Modul stehen daher Unterkategorien zur Verfügung, anhand derer eine Individuelle Anpassung der Kriterien an die jeweilige Online-Leistung möglich ist. Etwa werden in diesem Modul – je nach Funktion – spezifische Anforderungen für E-Health-Dienste, Online-Videosprechstunden, Presseportale, Bürgerportaldienste, Registrierungsvorgänge, Anmeldungen an Online-Accounts oder Online-Einwilligungsfunktionen geprüft.

M 3 Verbraucherschutz

Das (optionale) Modul Verbraucherschutz ergänzt speziell für Online-Shops und Online-Bestellvorgänge die Anforderungen an Datenschutz und Datensicherheit durch die spezifischen Vorgaben des Fernabsatzes (E-Commerce), wie etwa spezifische Informationspflichten und verbraucherfreundliche Umsetzung (Bestellvorgang, Widerrufsmöglichkeit, Rückabwicklung). Es wird nur geprüft, wenn entsprechende Dienste zur Verfügung gestellt werden.

M 4 Datenschutzmanagement

Das Modul Datenschutzmanagement beinhaltet die Organisation des geprüften Unternehmens mit Blick auf organisatorische und sicherheits-technische Maßnahmen. Hier ist zu prüfen, wie der Datenschutz beim Anbieter umgesetzt wird, ob und wie Auftragnehmer einer Datenverarbeitung in die Kontrolle einbezogen sind und wie die IT-Sicherheit bezogen auf die relevanten Online-Services umgesetzt wurden. Da das Datenschutzmanagement die Basis für die tatsächliche Umsetzung der rechtlichen Anforderungen darstellt, kommt dem Modul immer eine besondere Bedeutung zu.

M 5 Videosprechstunde

In Modul des Kriterienkatalogs werden die besonderen inhaltlichen Anforderungen an Anbieter von Online-Videosprechstunden beschrieben. Diese ergeben sich aus den Anforderungen der §§ 2und 5 der Anlage 31b zum Bundesmantelvertrag - Ärzte. Die Anforderungen dieses Moduls spiegeln die speziellen Anforderungen an Videodienste gemäß § 5 Abs. 2 wider.

3.2. Die Auswahl der Module für die Begutachtung

Der modulare Aufbau der internet privacy standards ermöglicht es, die Audit-Kriterien flexibel anzupassen, wenn eine Dienstleistung inhaltlich umgestellt, erweitert oder beschränkt wird. Darüber hinaus können Unternehmen die Einhaltung der Kriterien vorab selbst überprüfen. Allgemeingültige Module (M1, M2, M4) sind dabei immer einzubeziehen, während die Anwendung des spezifischen Moduls Verbraucherschutz M3 sich nach der Bestell-Funktion des Webportals richtet.

Beispiel: Für die Prüfung eines Online-Shops werden i.d.R. die Module Info-Abruf, Individual-Dienstleistung, Verbraucherschutz und Datenschutzmanagement angewandt. Für die Prüfung eines Webportals ohne E-Commerce-Funktionen die Module M1, M2 und M4.

Soweit sich die Module inhaltlich überschneiden, ist es zulässig, diese in einem Modul zusammenzufassen und in anderen Modulen darauf zu verweisen (z.B. kommen in allen Modulen Aspekte der Transparenz vor; hier kann auf die Ausführungen zu Modul M1 verwiesen werden.

Beispiel: Auf dem Webportal werden ein Registrierungsformular, ein User-Account sowie ein Online-Kontaktformular angeboten. In Modul M1 werden u.a. Impressum, Datenschutzerklärung sowie Umgang mit IP-Adresse, Cookies und Social-Plugins und die Verschlüsselung der Webformulare geprüft. In M2 werden die jeweiligen Online-Formulare nach und nach geprüft. Im Modul Datenschutzmanagement die Datenschutzorganisation des Anbieters sowie die von ihm getroffenen technischen und organisatorischen Datensicherheitsmaßnahmen.

4. Das Bewertungssystem

4.1. Die Punktevergabe

Für eine Vergabe des Gütesiegels nach ips sind mindestens zwei Punkte in der Gesamtwertung aller anwendbaren Module zu erreichen. Das Bewertungssystem sieht pro Kriterium eine Punktevergabe von null bis drei Punkten vor:

0 Punkte: die Anforderungen sind nicht erfüllt: diese Bewertung wird erteilt, wenn gesetzliche oder dem Stand der Technik entsprechende Anforderungen entweder überhaupt nicht oder nach dem Stand der Wissenschaft und Rechtsprechung unzureichend umgesetzt wurde. Es handelt sich um eine Abweichung von den geforderten Kriterien. Bei dieser Bewertung als nicht-konform kann insgesamt keine Vergabe des Gütesiegels erfolgen, auch wenn andere Aspekte im Audit besser bewertet wurden.

1 Punkt: die Anforderungen sind zwar noch konform umgesetzt, jedoch besteht aus Sicht der Auditoren Verbesserungsmöglichkeit. Diese Bewertung kann bei einer Bewertung eines anderen Aspektes des Moduls mit „3“ ausgeglichen werden.

2 Punkte: die Anforderungen sind adäquat / konform zu den Anforderungen erfüllt: diese Bewertung erfordert eine zum Audit-Zeitpunkt bereits erfolgte Umsetzung aller gesetzlichen und technischen Mindestanforderungen.

3 Punkte: die Anforderungen sind vorbildlich erfüllt: drei Punkte können vergeben werden, wenn das geprüfte Unternehmen über die gesetzlichen Erfordernisse hinaus weitergehende Anstrengungen unternommen hat, durch welche die Verbraucher- und Datenschutz-Belange unterstützt oder gefördert werden (privacy by design).

Dem Bewertungssystem liegt der Gedanke zugrunde, dass Verbesserungsmöglichkeiten bei einzelnen Aspekten mit überobligatorischer Umsetzung von Anforderungen bei anderen Aspekten ausgeglichen werden können. Dies soll ein Hilfsmittel sein, um den Gesamtkonformität des Webportals / Webservices zu den Anforderungen „messbar“ zu machen. Überall dort, wo gesetzliche Anforderungen nicht eingehalten werden, können Punkte aber erst vergeben werden, wenn die Abweichung beseitigt ist.

Beispiel: Ein Impressum, das die gesetzlichen Mindestangaben nicht enthält, kann erst dann mit zwei Punkten bewertet werden, wenn die fehlenden Angaben nachgeholt wurden. Auch die Vergabe nur eines Punktes ist vorher nicht möglich.

4.2. Die Gewichtung der Module

Das Bewertungssystem basiert neben der Punktevergabe auf dem Gedanken, dass die oben genannten Module unterschiedliche Gewichtung aufweisen. Die Gewichtung beruht auf der Schutzbedürftigkeit der in dem betreffenden Modul erhobenen und verarbeiteten Daten. Einbeziehung und Gewichtung von Modulen ist Aufgabe des Auditors und muss nachvollziehbar begründet werden.

Beispiel: Für einen Online-Shop sind die Module „Informations-Abruf", „Individual-Dienstleistung", „Verbraucherschutz" und „Datenschutzmanagement" anwendbar. Diese könnten z.B. mit 10% „M1", 15% „M2", 25% „M3" und 50% „M3" gewichtet werden, da es beim E-Commerce vor allem auf das grundsätzliche Datenschutzmanagement und den Verbraucherschutz ankommt, weniger jedoch auf die reinen Informationen der Webseite.

Eine Anmerkung zum Bewertungssystem: Die internet privacy standards sollen kein starres Korsett sein, in das eine Bewertung von Online-Dienstleistungen „hineingepresst" werden muss. Es soll vielmehr als Hilfsmittel zur Begutachtung dienen, um ein möglichst homogenes Niveau sowie eine Vergleichbarkeit der Umsetzung von rechtlichen und technischen Anforderungen zu schaffen. Jeder Auditor ist dabei aufgefordert, seine eigenen Kenntnisse und Erfahrungen einfließen zu lassen und wenn es in Einzelfällen erforderlich erscheint, von dem vorgegebenen Bewertungsraster – mit entsprechender Begründung - abzuweichen.

5. Der Ablauf eines Audits nach den internet privacy standards

5.1. Zusammenstellung und Gewichtung der Module

Im ersten Schritt wird das Webportal vom lizenzierten ips-Auditor gesichtet und die anwendbaren Module festgelegt. Im Anschluss erfolgt die Gewichtung der Module. Damit ist das „Prüfungsgerüst" erstellt.

5.2. Kriterienprüfung, Punktevergabe und Berechnung des Ergebnisses

Nun erfolgt die eigentliche Prüfung anhand der Kriterien und die Dokumentation der Ergebnisse. Die jeweils erreichten Punkte werden am Ende eines jeden Moduls zusammengezählt. Anhand der zuvor bestimmten Gewichtung wird aus den erreichten Punkten eine Durchschnittspunktzahl (Ø-Punktzahl) für das jeweilige Modul errechnet. Die Ø-Punktzahl wird sodann in Relation zu der festgelegten Gewichtung des Moduls gesetzt und daraus ein Punktanteil ermittelt.

Beispiel: im Durchschnitt wurden im Modul 1 insg. 2,71 Punkte erreicht. Gewichtet wird M1 mit 20 %. Der Anteil der Punkte beträgt daher 0,54 Punkte.

Anschließend wird der Punktanteil aller Module zusammengerechnet. Diese Gesamtpunktzahl muss mindestens den Wert „2“ ergeben, anderenfalls gilt die Auditierung als nicht bestanden. Die Berechnung kann in einer Übersicht dargestellt werden, die z.B. wie folgt aussieht:

MODUL INFO-ANGEBOT	PUNKTE
Anbieterkennzeichnung	3
Datenschutzerklärung	3
Weiterleitung	2
Verantwortung f. Inhalte	2
Nutzungsdatenumgang	3
Kommerzielle Kommunikation	3
Datenvermeidung/-sparsamkeit	3
Gesamtpunkte/Maximalpunkte	19/21
Ø - Punktzahl	2,71
Gewichtung	10 %
Punktanteil M1	0,54
MODUL INDIVIDUALLEISTUNG	**PUNKTE**
Transparenz	3
materielle Voraussetzungen	2
Datenvermeidung/-sparsamkeit	2
Technisch-organisat. Sicherheit	3
Gesamtpunkte/Maximalpunkte	10 / 12
Ø - Punktzahl	2,5
Gewichtung	15 %
Punktanteil M2	0,375
Modul Datenschutzmanagement	**PUNKTE**
Betriebl. Datenschutzbeauftragte	3
Auftragskontrolle	2
Verfahrensverzeichnis	3

Datenschutzorganisation	3
Techn.-org. Sicherheit	3
Umsetzung von Betroffenenrechten	3
Gesamtpunkte / Maximalpunkte	17 / 18
Ø - Punktzahl	2,83
Gewichtung	45%
Punktanteil M4	1,274
Modul Videosprechstunden	**PUNKTE**
Peer to Peer	2
Ort der Datenverarbeitung	2
Ende-zu-Ende-Verschlüsselung	2
Gesamtpunkte/Maximalpunkte	6 / 9
Ø - Punktzahl	2,000
Gewichtung	35 %
Punktanteil M3	0,7
Gesamtpunktergebnis	2,620

5.3. Dokumentation / Auditreport

Die Dokumentation (Audit-Report) muss – auch zur Erleichterung des Prüf-Aufwands der Vergabestelle – den Aufbau des Kriterienkataloges berücksichtigen, wobei ansonsten jedoch keine weitere Form vorgegeben ist. Im Audit-Report müssen die gefundenen Ergebnisse sowohl mit den aufgefundenen Abweichungen oder Empfehlungen aber auch mit den vorbildlichen Umsetzungen dargestellt werden. Dabei können auch Abbildungen der Web-Funktionen (z.B. Screenshots) hilfreich sein. Soweit negative Bewertungen erfolgen, müssen diese besonders begründet werden.

Der Audit-Report endet mit einer Empfehlung gegenüber der Vergabestelle, das ips Gütesiegel zu erteilen oder nicht.

Ferner erstellt der ips-Auditor einen Entwurf für ein Kurzgutachten zur Vorlage bei der Vergabestelle. Dieses dient dazu, dem Nutzer des Web-Angebotes die Prüfergebnisse im Überblick zu erläutern. Auf den Webseiten www.datenschutz-cert.de ist hierzu ein Informationsblatt mit Anforderungen an das Kurzgutachten abrufbar. Das Kurzgutachten wird von der Vergabestelle ergänzt und bei erfolgreicher Vergabe des Gütesiegels veröffentlicht.

6. Vergabe des ips-Gütesiegels und Veröffentlichung des Ergebnisses

Die Vergabestelle der datenschutz cert GmbH prüft den Audit-Report des lizenzierten ips-Auditors auf Schlüssigkeit. Kommt auch sie zu dem Ergebnis, dass das Webportal alle Anforderungen der ips-Kriterien mit einer Gesamtnote von mindestens 2 Punkten umsetzt, wird das Gütesiegel erteilt. Die Vergabestelle kann allerdings auch von der Ansicht des ips-Auditors abweichen und das Gütesiegel nicht erteilen, was dann seitens der Vergabestelle zu begründen ist.

Die Vergabestelle kann das ips-Gütesiegel erteilen. Hierzu wird zum einen das ips-Logo auf der Homepage (mindestens auf der Startseite) implementiert und mit einem Link versehen, über den Interessierte per Klick zum online bereitgestellten Kurzgutachten gelangen können. Das Kurzgutachten ist auf dem Server der datenschutz cert GmbH abgelegt und innerhalb des geprüften Angebotes mit dem ips-Logo verlinkt. Das ips-Logo, die Kriterienkataloge sowie Marke und Hinweise auf ein gültiges ips-Gütesiegel dürfen nur mit Genehmigung der Vergabestelle und auf der Grundlage der Vergabe- und Nutzungsbedingungen verwendet werden.

Das Gütesiegel ist bei gleichbleibendem Webangebot für einen Zeitraum von zwei Jahren gültig und kann nach Ablauf der Gültigkeit durch eine erneute Prüfung mit positivem Abschluss erneuert werden.