ADV-Arbeitsgemeinschaft
Geschäftsstelle im Ministerium für
Arbeit, Gesundheit und Soziales
des Landes Nordrhein-Westfalen

Leitfaden zur Prüfung eines Internetauftritts

Änderungshistorie

Version	Datum	Bearbeitungsstand	Bearbeitung durch
0.1	10.04.2015	Neuanlage	Hamsch
1.0	22.06.2015	Einsatzbereit für alle Themenbereiche Fachliche Qualitätssicherung noch ausstehend	Hamsch
1.1	24.07.2015	Redaktionelle Änderungen nach QS, kleinere Korrekturen	Hamsch
1.2	19.12.2015	Fehlerbehebung, Ergänzungen	Hamsch
1.3	03.2016	Ergänzungen nach Workshop (Kapitel 1.1 – Verträge, 6.1.1 – Softwareentwicklung)	Hamsch Pahmeyer Hamsch
1.4	16.06.2016	Überarbeitung und Erstellung des Dokumentes „Leitfaden zur Prüfung eines Internetauftrittes“ inkl. ausgewählter Checklisten zum Zwecke der Veröffentlichung	Hamsch
1.5	13.10.2016	Ergänzungen nach Workshop	Hamsch
1.6	16.05.2018	Überarbeitung redaktionell sowie Abschnitt 6.1.3.1.2 (Kennwörter), Kap. 5 (Datenschutz-grundverordnung DSGVO)	Hamsch

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Inhalt

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

VORWORT

In diesem Prüfleitfaden werden Hinweise auf Schwachstellen in Webseiten und Umgehungsmöglichkeiten der Sicherheitsmaßnahmen gegeben. Bei der Prüfung eines Internetauftritts ist zu beachten, dass das reine Eindringen in ein System straffrei ist. Manipuliert der Eindringling aber hierbei Daten oder verschafft sich besonders gesicherte Daten, so kommt eine Strafbarkeit nach § 202 a StGB oder § 303 a StGB in Betracht. Die rechtlichen Grundlagen sind im „Technischen Handbuch Internet“ zu finden.
Im Zuge eines Tests auf möglichen Sicherheitslücken würden Handlungen ausgeführt die, wenn sie nicht mit der Einwilligung der Auftraggebenden geschehen, gegen geltende Gesetze verstoßen können (z. B. Ausprobieren von Standardkennwörtern oder SQL-Abfragen und - bei Erfolg - Zugriff auf geschützte Bereiche). Aus diesem Grund sind genaue technische Anleitungen oder Codebeispiele kein Bestandteil dieser Prüfhilfe.

Es wird dringend empfohlen, eventuelle Prüfungen auf Sicherheitslücken nur durch die Betreibenden des Internetauftritts bzw. durch deren externe Beauftragte durchführen zu lassen. Während dieser Prüfung sollten alle Handlungen nachvollziehbar dokumentiert werden (Methode/Durchführung/Ergebnis).

Um die Sicherheit einer Webseite, einer Onlinegeschäftsstelle oder einer ganzen Internetpräsenz beurteilen zu können, ist es aus Sicht der ADV-AG notwendig, einen professionellen Penetrationstest durch externe Tester durchführen zu lassen. Dieser Test kann durch die Krankenkasse veranlasst werden, aber auch der Softwareentwickler kann diesen auf einer dokumentierten Konfiguration durchführen.

Der Nachweis eines Penetrationstests der aktuellen Softwareversion sowie die Dokumentation der Behebung eventuell gefundener Schwachstellen ist aus Sicht der ADV-AG als Nachweis einer weitgehend gesicherten Webseite (gem. Kapitel 6/7) ausreichend.

Vor Beginn der Prüfung
Es ist sinnvoll, vor Beginn der Prüfung die Ansprechpartner bei der zu prüfenden Institution zu ermitteln. Je nach Organisation der Institution werden die Internetseiten durch Dienstleister oder selbst betrieben. Die Gestaltung (in der Regel über ein Content-Management –System) kann durch die IT- oder die Fachabteilung erfolgen. Automatisierte Verfahren wie Dateneingänge werden meist durch den Softwareentwickler realisiert. In Abhängigkeit von den Prüfthemen sind im Verlauf der Prüfungen die vertraglichen Regelungen zu betrachten.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ZIEL / AUFBAU DES PRÜFLEITFADENS

Ziel dieses Prüfleitfadens ist eine strukturierte Kurzprüfung des Internetauftritts eines Trägers der Sozialversicherung mit Unterstützung durch Checklisten, die diesem Dokument angehängt sind. Die Checklisten sind so formuliert, dass die Beantwortung einer Frage mit „**Nein**“ eine weitere Prüfung/Nachfrage bei der zu prüfenden Institution bzw. eine Prüfbemerkung erfordert. Die ersten Themen dieses Prüfleitfadens können problemlos auch ohne Vorkenntnisse geprüft werden, zum Ende werden die Themen technisch anspruchsvoller. Um sich an das Themengebiet und die Nutzung der Checklisten zu gewöhnen, wird empfohlen, die Themen in der Reihenfolge dieses Prüfleitfadens zu bearbeiten.

Aufgrund der sich schnell ändernden rechtlichen und technischen Anforderungen soll in diesem Prüfleitfaden keine Unterstützung zum Berichtsaufbau gegeben werden. Hilfestellung leistet jedoch das Dokument „Technisches Handbuch Internetauftritt“, welches zusammen mit diesem Prüfleitfaden ausgeliefert wird. Die aktuelle Version steht zudem auf der Infobörse der Prüfdienste zum Download bereit. Im „Technischen Handbuch Internetauftritt“ sind Rechtsgrundlagen sowie weitere Informationen und Hintergründe zu den in diesem Leitfaden aufgeführten Prüffragen enthalten. Zu den Prüfthemen wird jeweils ein Verweis auf das entsprechende Thema im „Technischen Handbuch Internetauftritt“ aufgeführt. Zudem erläutert im „Technischen Handbuch Internet“ ein umfangreiches Glossar viele technische Fachbegriffe. Die hier verwendeten und im Glossar zu findenden Begriffe sind durch dieses Symbol gekennzeichnet.

Geprüft werden die Belange des Datenschutzes und der Datensicherheit bei der Gestaltung bzw. Nutzung des Internetauftrittes sowie die im Prüfthemenkatalog (s. u.) unter Punkt 4.5 genannten Themen. Neben den Normen zum Datenschutz sind auch die allgemein anerkannten Regeln zur Gestaltung von Internetseiten sowie der aktuelle Stand der Maßnahmen zur Gewährleistung der Sicherheit eines Internetauftritts zu berücksichtigen.

<u>Prüfthemenkatalog</u>

Kapitel	4	Verwaltung
Abschnitt	4.5	Öffentlichkeitsarbeit und Repräsentation
Unterabschnitt	4.5.1	Operatives Marketing

4.5.1.X Internetauftritt / Internetangebote

Die inhaltliche Prüfung des Internetauftritts sowie Fragen zum Inhalt einer Onlinegeschäftsstelle sind nicht das Ziel dieses Prüfleitfadens. Zur Prüfung einer Onlinegeschäftsstelle wird auf den „Leitfaden Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten“ verwiesen. Dieser stellt die gesetzlichen Anforderungen zu dieser Thematik sowie die hieraus abgeleiteten Anforderungen der Prüfdienste für die praktische Umsetzung dar.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

1 VERTRAGLICHE VORAUSSETZUNGEN

Die zu prüfenden Institutionen schließen im Laufe ihrer Geschäftstätigkeit eine Vielzahl von Verträgen ab. In einem Softwarevertrag sind die Interessen des Auftragnehmers und Auftraggebers abschließend zu regeln. Neben der genauen Beschreibung des zu erstellenden Produktes sind Vereinbarungen über den erwarteten Qualitätsstandard, den Fertigstellungstermin, die Installationsvorgaben der Software, die Nutzungsrechte, die Einweisung in die Software, die Abnahme, den Quellcode und die Bezahlung zu treffen.

Die nachfolgende Checkliste wurde aus den verschiedensten Musterverträgen, die im Internet zu Softwareverträgen verfügbar sind, entwickelt. Ein Anspruch auf Vollständigkeit und Richtigkeit besteht nicht und die Liste kann nur als Leitfaden bzw. Anregung für ihre Prüfungen dienen. Sie beinhaltet Fragen zu den Punkten, die die typischen Interessenlagen von Auftragnehmer und Auftraggeber im Rahmen der Softwareentwicklung betreffen und mindestens in einem Vertrag enthalten sein sollten.

Sollten sie anhand des ihnen vorliegenden konkreten Vertrages und der zu entwickelnden Software der zu prüfenden Institution weiteren Regelungsbedarf für nötig halten, führt dies zu einer Ausweitung der Prüfung / Beratung.

Zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

2 GESTALTUNG DER WEBSITE

Was erwarten Besucherinnen und Besucher von einer Webseite?

- Aktualität und Information (nützlich, relevant, tagesaktuell)
- Einfache Bedienung (keine Inhalte, die mehr als Standardsoftware benötigen)
- Funktionales Design (mediengerecht und unterstützend)
- Geringe Antwort- und Ladezeiten
- Klare Benutzerführung (Wo befinde ich mich? Wie komme ich zurück?)
- Kurze Wege (mit „2 Klicks“ zu den relevanten Informationen!)
- Funktionale Suchfunktion (bei Eingabe eines Suchbegriffs werden Treffer angezeigt – auch wenn der Suchbegriff nicht buchstabengenau übereinstimmt. Z. B. Suchbegriff: *Bericht*, Treffer: Prüf*bericht*)
- Transparenz (Wer, was und wo auf einen Blick!)

Im ersten Schritt kann die Revision die Einhaltung der grundlegenden Gestaltungsregeln für Internetseiten durch Inaugenscheinnahme leicht selbst prüfen. Informationen sind im „Technischen Handbuch Internetauftritt“ unter dem Stichwort „1.0 Gestaltung einer Webseite“ zu finden. Eine Checkliste mit Prüffragen ist in der Anlage 1 dieses Dokumentes zu finden.

Grundsätzlich ist die gute Vorbereitung und Konzeption einer Webseite der erste Schritt für eine erfolgreiche und zielgruppenorientierte Präsenz im Internet. Hierzu empfehlen sich methodische Schritte bei der Erstellung eines Konzeptes, die auch im Rahmen einer Prüfung nachvollzogen werden können. Vor Erstellung einer Webseite sind viele Fragen zu beantworten. Hier einige Beispiele:

- Welches Ziel soll durch die Webseite erreicht bzw. unterstützt werden?
  - Marketing
  - Kundenpflege und Kundenbindung
  - Zugang auf Onlinegeschäftsstelle
- Was sind die möglichen Inhalte der Webseite, welche sind vorhanden, welche müssen noch erstellt werden?
  - Kundenzeitschrift
  - Bonusprogramme
  - Versionen für mobile Geräte
  - Angebot von Downloads
- Welche finanziellen und personellen Ressourcen stehen für die Realisierung und zum Betreiben zur Verfügung?
  - Kosten- / Nutzen Analyse
  - Wirtschaftlichkeit

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

- An welche Zielgruppe soll sich das Webangebot richten? Sind diese Zielgruppen sehr unterschiedlich, sollte eine Priorisierung anhand der Marketingstrategien oder Unternehmensziele vorgenommen werden.
    - welche Inhalte erwartet die Zielgruppe?
    - welche Sprache bzw. Ansprache erwartet die Zielgruppe?
    - über was für Kompetenzen im Umgang mit Webseiten verfügt die Zielgruppe?
    - welche technische Ausrüstung ist bei der Zielgruppe vorhanden?
- Welche weiteren Voraussetzungen müssen erfüllt / geklärt werden?
    - Zuständigkeiten für Aktualisierungen klären
    - Systemvoraussetzungen / Kontakte mit Anbietern, Rechenzentren
    - (ggf. Entwurf einer) Corporate Identity
    - Skalierbarkeit
    - Performance, Verfügbarkeit
    - …

Wenn diese (und andere) Fragen geklärt sind, könnte die Webseite „am grünen Tisch“ entworfen werden. Folgende Punkte könnten hier schon berücksichtigt werden, z.B.:

- Inhalt und Inhaltspräsentation,
- grafische Gestaltung,
- Funktionsumfang und Features,
- Aktualität,
- technische Realisierung,
- Suchmaschinenplatzierung und benutzte Suchwörter (Keywords),
- Verlinkung (wer verweist auf die Webseite),
- besondere Alleinstellungsmerkmale.

Bereits an dieser Stelle kann der grundsätzliche Aufbau der Webseite festgelegt werden, der dann über die spätere Akzeptanz, Nutzerfreundlichkeit usw. entscheidet.

Die Gestaltung einer Internetseite obliegt ausschließlich den Betreiberinnen und Betreibern. Oft ist es schwierig, eine Begründung für eine Umgestaltung zu finden. Letztlich bringt aber eine unübersichtliche und/oder nur wenig genutzte Internetseite keinen Vorteil für die Betreibenden. Hier könnte also mit einer fehlenden Wirtschaftlichkeit argumentiert werden.

Zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

3 BARRIEREFREIHEIT

Webseiten barrierefrei zu gestalten bedeutet einzuplanen, dass Menschen mit unterschiedlichen Fähigkeiten und Voraussetzungen, unterschiedlicher Hard- und Software und auch unterschiedlichen Browsereinstellungen auf Internetseiten zugreifen können. Grundlage hierfür ist z. B. die „Barrierefreie Informationstechnik-Verordnung — BITV 2.0“ .

Nach § 11 Behindertengleichstellungsgesetz müssen Träger öffentlicher Gewalt ihre Internetauftritte und –angebote so gestalten, dass sie von behinderten Menschen grundsätzlich uneingeschränkt genutzt werden können.

Mit der Checkliste in der Anlage 2 können einige Merkmale einer barrierefreien Webseite durch die Revision schnell bewertet werden. Hintergrundinformationen sind im „Technischen Handbuch Internetauftritt“ zu finden. Genaue Erklärungen zu jeder Prüffrage und die entsprechenden Verweise auf die Anforderungen der *BITV* sind Beispielsweise im BITV-Test zu finden. *(*Der BITV-Test ist ein Prüfverfahren für die umfassende Prüfung der Barrierefreiheit von informationsorientierten Webangeboten www.bitvtest.de).

Die Prüffragen in der Checkliste sind bewusst einfach gehalten und auch ohne technische Kenntnisse oder Programmierkenntnisse zu beantworten. Hierdurch bedingt können nicht alle Aspekte einer barrierefreien Webseite bewertet werden. Da der Begriff Barrierefreiheit sich auf die unterschiedlichsten Einschränkungen (siehe auch technisches Handbuch Internet) und deren Berücksichtigung auf einer Webseite bezieht, würde eine umfassende Prüfung den Umfang der Checklisten übersteigen. Es empfiehlt sich, die Prüfung der Barrierefreiheit eines Internetauftritts gesondert vorzunehmen oder entsprechende elektronische Testwerkzeuge (siehe BITV-Test) zu verwenden.

zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

4 RECHTLICHE VORAUSSETZUNGEN BEIM BETRIEB EINER WEBSEITE

Ein Teil der rechtlichen Anforderungen an den Betrieb einer Webseite ist aus dem Telemediengesetz (TMG) abzuleiten. Die Checkliste in der Anlage 3 kann teilweise von der Revision ausgefüllt werden, einige Fragen erfordern eine Beantwortung der Webseitenbetreiber. Diese sind gesondert aufgeführt.

4.1 Namens- / Markenrechte an der Domain

Die Domain darf keine Rechte Dritter verletzen. Die bloße Registrierung einer Domain führt nicht dazu, dass der Inhaberin bzw. dem Inhaber an der Bezeichnung selbst irgendwelche Rechte zustehen. Es muss im Vorfeld durch den Registrateur selbst geprüft werden, ob der Domainname Rechte Anderer verletzt. Nach § 12 BGB genießen sowohl bürgerliche Namen, die Firma (der Name eines Unternehmens) als auch Berufsbezeichnungen und Pseudonyme Schutz vor unbefugter Verwendung durch Dritte.
Vor allem bei Unternehmensnamen (der Firma) kann es im Fall der Gleichnamigkeit zu Streitigkeiten kommen. Zunächst gilt das Prioritätsprinzip: Wer die Domain zuerst registriert hat, kann diese Domain auch nutzen. Hier muss dann aber geprüft werden, ob nicht einer Firma ein so genanntes „besseres Recht“ an dieser Bezeichnung zukommt. Dieses bessere Recht kann sich ergeben aus dem Namens-, Marken- oder Wettbewerbsrecht.

4.2 Die Inhalte

Nahezu alles, was sich im Netz finden lässt, kann urheberrechtlich geschützt sein. Hierzu zählen (mit Unterschieden im Detail) insbesondere Texte, Bilder, Stadtpläne sowie Fotos und Videos. Auf eine Webseite sollten keine fremden Inhalte übernommen werden, ohne das eine ausdrückliche Zustimmung der jeweiligen Urheber eingeholt und entsprechende Lizenzverträge abgeschlossen wurden. Ob ein selbst genutztes Bild auf einer anderen Webseite ebenfalls präsentiert wird, lässt sich leicht (z.B. mit der Google-Bildersuche) feststellen.
Verträge über Nutzungsrechte an Inhalten sind schriftlich abzuschließen und müssen konkreten Bezug auf die Inhalte, an denen Nutzungsrechte übertragen werden sollen, beinhalten. Es ist durch den Sozialversicherungsträger zu prüfen, ob die Vertragspartner (z. B. Webdesign-Agentur) tatsächlich selbst über die notwendigen Rechte verfügen, die übertragen werden sollen.

4.3 Impressum

Nach § 5 TMG sind folgende Informationen auf einer Internetseite – leicht erkennbar und unmittelbar erreichbar – vorzuhalten:

- Name und Anschrift, unter der die Inhaber niedergelassen sind, bei juristischen Personen zusätzlich die Rechtsform, den Vertretungsberechtigten und, sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen,
- Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit den Seiteninhabern ermöglichen, einschließlich der Adresse der elektronischen Post,
- Angaben zur zuständigen Aufsichtsbehörde, soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf,
- das Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das die Seiteninhaber eingetragen sind, und die entsprechende Registernummer.

4.4 Mitgliederzeitschrift online: Angaben bei journalistisch-redaktionell gestalteten Angeboten (z. B. Mitgliederzeitschrift)

Anbieterinnen und Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten, in denen insbesondere vollständig oder teilweise Inhalte periodischer Druckerzeugnisse in Text oder Bild wiedergegeben werden, haben nach § 55 Abs. 2 Rundfunkstaatsvertrag (RStV) zusätzlich eine verantwortliche Person mit Angabe des Namens und der Anschrift zu benennen. Werden mehrere Verantwortliche benannt, so ist kenntlich zu machen, für welchen Teil des Dienstes die jeweils Benannten verantwortlich ist. Als Verantwortliche bzw. Verantwortlicher darf nur benannt werden, wer
- seinen ständigen Aufenthalt im Inland hat,
- nicht infolge Richterspruchs die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat,
- voll geschäftsfähig ist und
- unbeschränkt strafrechtlich verfolgt werden kann.

4.5 Allgemeine rechtliche Hinweise / Haftungsausschluss (Disclaimer)

Weit verbreitet in vielen Internetauftritten ist die Nutzung eines sog. Disclaimer, der die Haftung der Webseitenbetreibenden für die verlinkten Inhalte einschränken soll. Die Idee des Disclaimer beruht auf einem Urteil des LG Hamburg (Mit Urteil vom 12. Mai 1998 – 312 O 85/98 – „Haftung für Links“ hat das Landgericht (LG) Hamburg entschieden, dass man durch das Setzen eines Links, die Inhalte der gelinkten Seite ggf. mit zu verantworten hat. Dies kann – so das LG – nur dadurch verhindert werden, dass man sich ausdrücklich von diesen Inhalten distanziert). Die Problematik der rechtlichen Bewertung für in Webseiten verlinkte Inhalte ist zur Zeit noch nicht abschließend geklärt. Einigkeit besteht darin, dass ein Disclaimer auf einer Webseite nicht dazu geeignet ist, sich von allen verlinkten Inhalten zu distanzieren. Im Hinblick auf die umstrittene Einordnung von Hyperlinks unter §§ 7 Abs. 1, 8 oder 10 TMG kann es im Einzelfall jedoch darauf ankommen, ob sich die Webseitenbetreibenden auf der Homepage den fremden Inhalt zu Eigen machen oder ob sie sich hinreichend deutlich von den externen Inhalten distanzieren. Ein entsprechender Hinweis, dass es sich bei den „verlinkten“ Inhalten um Angebote Dritter handelt, kann zumindest deklaratorisch (im Sinne einer inhaltlichen Abgrenzung von fremden Inhalten) wirken. Entscheidend sind allerdings die objektiven

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Umstände, insbesondere die äußere Gestaltung der Homepage (z. B. Frames, Verwendung von Inline-Links (Verweise innerhalb der Webseite)) und die inhaltliche Einbeziehung des Inhalts, bei deren Bewertung ein Disclaimer nur eines von vielen Kriterien darstellt.
Daher kann durch einen Disclaimer nicht ausgeschlossen werden, dass sich die Urheber eines Hyperlinks, der auf strafbare fremde Inhalte verweist, selbst strafbar machen, wenn sie die fremden Inhalte kannten und insofern vorsätzlich handelten (z. B. wegen Beihilfe zur Verbreitung pornographischer Inhalte bei bewusster Verlinkung auf solche Inhalte).

zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

5 DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

Die am 25.05.2018 in Kraft tretende Datenschutzgrundverordnung (DSGVO) enthält den rechtlichen Rahmen zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Natürliche Personen sollten hierdurch die Kontrolle über ihre eigenen Daten besitzen. Zudem sollen natürliche Personen, Wirtschaft und Staat in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.

Artikel 5 der DSGVO sind die Grundsätze der Verarbeitung personenbezogener Daten zu entnehmen (s. auch 5.1.5):

- Rechtmäßigkeit, Transparenz
- Zweckbindung
- Datensparsamkeit
- Richtigkeit
- nachvollziehbare Zeitliche Bindung der Speicherdauer an den Erhebungszweck
- Integrität und Vertraulichkeit

In den Erwägungsgründen zu Artikel 5 DSGVO (EG 39) werden die Grundsätze zur Verarbeitung personenbezogener Daten u.a. wie folgt erläutert:

„…Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind….

…Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen….

…Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen….

…Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können….“

5.1 Schutz personenbezogener Daten durch die DSGVO

5.1.1 Einwilligung (Art. 7 DSGVO)

Die Einwilligung der Nutzer einer Internetseite zur Speicherung personenbezogener Daten muss aktiv erfolgen und eindeutig sein. Dieses setzt voraus, dass vorausgehende Erklärungen und Erläuterungen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Aus der Aufforderung zur Einwilligung muss unmissverständlich zu erkennen sein, welche Dienste auf die personenbezogenen Daten Zugriff erhalten und welche Art von Daten verarbeitet, gespeichert, weitergeleitet und genutzt werden.

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Vorgang des Wiederrufes ist ebenso einfach zu gestalten wie die Einwilligung. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die Person ist von den Auswirkungen des Widerrufes in Kenntnis zu setzten.

5.1.2 Technische und organisatorische Maßnahmen

Art. 32 DSGVO nennt in Verbindung mit § 64 DBSG(neu) die Anforderungen im Bezug auf technisch/organisatorische Maßnahmen zur Wahrung der Sicherheit der Datenverarbeitung. Während die DSGVO eher allgemein gehaltene Grundsätze formuliert, nennt das BDSG (neu) konkrete Maßnahmen, die nach Durchführung einer Risikobewertung umzusetzen sind. Diese sind im einzelnen:

- Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort usw. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern.
- Datenträgerkontrolle: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern. Die Daten sind z. B. ausschließlich auf einem bestimmten Laufwerk eines Servers, Laptop/PC gespeichert, der gesichert und unter Kontrolle der Verantwortlichen verwahrt wird.
- Speicherkontrolle: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.
- Benutzerkontrolle: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte. D. h. durch die Administration werden nur die notwendigen Benutzerrechte vergeben, um die erforderlichen Aufgaben zu erfüllen.
- Zugriffskontrolle: Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer

Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. D. h. alle Regelungen, die dafür sorgen sollen, dass nur Berechtigte Einblick in Daten erhalten und diese nur ihrer Berechtigung entsprechend nutzen können.

- Übertragungskontrolle: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Hierzu gehört z. B. das Einrichten gesicherter Leitungen, die Dokumentation der Datenempfänger inkl. der Übermittlungs- und Löschfristen oder die Dokumentation der regelmäßigen Datenabrufe und – übermittlungen.
- Eingabekontrolle: Es muss nachträglich überprüft und festgestellt werden können, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind. Somit ist die verantwortliche Stelle angehalten, die Erhebung, Verarbeitung und Nutzung von solchen Daten umfassend zu protokollieren und diese Protokolle ihrerseits im Sinne von Verfügbarkeit, Integrität usw. zu sichern.
- Transportkontrolle: Bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern ist die Vertraulichkeit und Integrität der Daten zu schützen. Bei der Übermittlung elektronischer Daten sind diese z. B. durch Verschlüsselung zu schützen. Bei Transport von Datenträgern (aber auch von Akten) sind diese auf geeignete Weise vor Verlust und unbefugter Kenntnisnahme zu schützen.
- Wiederherstellbarkeit: Es ist sicherzustellen, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Die kann z.B. durch redundant eingesetzte Systeme und Bereitstellung von Ersatzhardware erfolgen, beinhaltet aber auch die Dokumentation von Hard- und Software, Datensicherungskonzepte sowie Wideranlaufpläne für die eingesetzten Systeme.
- Zuverlässigkeit: Es müssen alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Es ist z.B. über ein Monitoring der Systeme und deren Komponenten sicherzustellen, dass alle Funktionen zur Verfügung stehen. Weiterhin kann durch Systemüberwachung ein Angriff auf die Ressourcen z.B. durch Computerviren oder DDOS-Attacken frühzeitig festgestellt und unterbunden werden.
- Datenintegrität: Es ist zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden. Hierbei ist nicht ausschließlich eine systemseitige Fehlfunktion bei der Übertragung oder in der Hard- und Software auszuschließen. Auch Benutzer, die Ihre Systemprivilegien missbrauchen (Externe, aber auch Interne Benutzer) können Daten manipulieren.
- Auftragskontrolle: Alle personenbezogenen Daten, die an Dritte zur Verarbeitung weitergeleitet werden, sind ausschließlich nach den Weisungen des Auftraggebers zu verarbeiten. Die Ordnungs- und Weisungsgemäße Verarbeitung des Auftragsnehmers ist regelmäßig durch den Auftraggeber zu überwachen, bzw. zu kontrollieren. Die Kontrollrechte sind bei der Auftragsvergabe vertraglich zu vereinbaren.
- Verfügbarkeitskontrolle: Personenbezogene Daten sind vor Verlust und zufälliger Veränderung und Zerstörung zu schützen. Die Maßnahmen zur Verfügbarkeitskontrolle betreffen sowohl den Schutz gegen die physische Zerstörung der Datenverarbeitungsanlagen oder Diebstahl derselben als auch

weiter Maßnahmen, z.B. gegen Schadsoftware. Gegen äußere Einflüsse wie Feuer, Wasser oder Diebstahl können sowohl bauliche Maßnahmen als auch geeignete Datensicherungskonzepte wie redundante Datenhaltung schützen. Hierzu sind entsprechende Konzeptionen wie z.B. Backup – und Virenschutzkonzepte oder Notfallpläne zu erstellen und regelmäßig zu aktualisieren.

- Trennbarkeit: Das Trennungsgebot soll gewährleisten, dass Daten ausschließlich zu dem Zweck verarbeitet werden dürfen, zu dem sie auch erhoben worden sind. Hierbei soll sichergestellt werden, dass Daten von Betroffenen Personen nicht vollumfänglich ausgewertet werden und hierdurch die Persönlichkeitsrechte unzulässig beeinträchtigt werden. Voraussetzung für die Umsetzung des Trennungsgebotes ist, dass jedes einzelne Datum bzw. jede Klasse von Daten nach Herkunft oder Erhebungszweck kenntlich gemacht werden. Am Erhebungszweck von Daten lassen sich ggf. auch deren Löschfristen ableiten. Eine Konsequenz des Trennungsgebotes ist auch die zwingende Trennung von Test- und Produktivsystemen.

5.1.3 Speicherung von IP-Adressen

Über die Erhebung technischer Daten mit Personenbezug, z.B. IP-Adressen, die bei Besuch einer Internetseite automatisiert protokolliert werden, sind die Nutzer zu informieren. Ggf. sind diese zu löschen, sofern eine Einwilligung zur Speicherung nicht erfolgt oder widerrufen wird. (siehe hierzu auch EG 30 zur DSGVO).

Grundsätzlich ist eine Speicherung von IP-Adressen durch Webseiten-Anbieter und Onlinedienste nur zulässig, wenn die Funktionsfähigkeit dieses Dienstes nur so sichergestellt werden kann, der Webseiten-Betreiber ein berechtigtes Interesse daran hat und eine Abwägung der Interessen des Nutzers und des Webseiten-Betreibers ergibt, dass das Interesse des Webseiten-Betreibers überwiegt. Es muss folglich bei jeder Speicherung eine auf den Einzelfall gerichtete Interessenabwägung erfolgen. Für Anwendungen wie Webanalysen oder Werbung dürfen diese IP-Adressen nicht ohne explizite Zustimmung genutzt werden.

5.1.4 Verarbeitung besonderer Kategorien personenbezogener Daten und Gesundheitsdaten

Die Verarbeitung besonders sensibler personenbezogener Daten ist nach Art. 9 (1) DSGVO untersagt, sofern keine Ausnahme nach den Absätzen 2-4 i.V.m. §22 BDSG (neu) vorliegt.

Sofern besondere Kategorien personenbezogener Daten – z.B. Gesundheitsdaten verarbeitet werden, sind angemessene und spezifische Maßnahmen nach §22 BDSG (neu) zur Wahrung der Interessen der betroffenen Personen vorzunehmen. Die Notwendigkeit und Angemessenheit dieser Maßnahmen lässt sich nur dann bewerten, wenn eine Risikoanalyse durchgeführt wird. Aufgrund der gewonnenen Erkenntnisse über die Risiken (Schadensauswirkungen und Eintrittswahrscheinlichkeit) sind für alle erhobenen Datenarten die angemessenen und erforderlichen Maßnahmen abzuschätzen. Hierbei ist darauf zu achten, dass regelmäßig der Bestand der erhobenen Daten daraufhin

überprüft wird, ob sich mögliche Risiken, Schutzklassen oder Datenkategorien geändert haben.

5.1.5 Rechte aus der DSGVO

Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Durch die Fassung der DSGVO ist beabsichtigt, den Schutz personenbezogener Daten – im Einklang mit allen weiteren Grundrechten – ungeachtet der Staatsangehörigkeit und des Aufenthaltsortes auf dem Gebiet der EU zu gewährleisten. Trotz der immer schneller werdenden Entwicklung elektronischer Datenerfassungs- und austauschverfahren soll EU - weit ein hohes Datenschutzniveau gewährleistet werden. Um das Vertrauen der Nutzerinnen und Nutzer in den Umgang mit personenbezogenen Daten zu bestärken, wurden in die DSGVO (Kapitel 3, Artikel 12-23) nachfolgende Rechte der betroffenen Personen festgeschrieben:

5.1.5.1 Information

Die betroffenen Personen sollen transparent, präzise und leicht verständlich darüber unterrichtet und aufgeklärt werden, dass eine Verarbeitung personenbezogener Daten stattfindet, welchen Zweck diese dient und welche personenbezogenen Daten davon betroffen sind. Sofern aufgrund dieser Daten ein Profiling, also eine automatisierte Bewertung des Datenprofils stattfindet, ist die betroffene Person darüber zu informieren und muss ggf. zu einer Zustimmung zum Verfahren aufgefordert werden.

Wenn eine Verarbeitung sich an Kinder richtet, sind Informationen in einer einfachen und klaren Sprache so bereit zu stellen, dass diese sie verstehen und bewerten können.

5.1.5.2 Transparenz

Bereits zum Zeitpunkt der Erhebung personenbezogener Daten muss der Verantwortliche der betroffenen Person nach Art. 13 DSGVO Details zu den Verantwortlichen und der beabsichtigten Verwendung der Daten bekannt geben. Darüber hinaus sind der betroffenen Person weitere Einzelheiten zur Kenntnis zu geben, z.B. die geplante Speicherdauer, Beschwerde- und Informationsrechte sowie das Recht auf Widerruf und/oder Löschung der erhobenen Daten.

5.1.5.3 Auskunft

Neben der Informationspflicht die der Verantwortliche gegenüber der betroffenen Person bei der Erhebung der Daten hat, besteht auch ein Auskunftsrecht der betroffenen Person nach Art. 15 DSGVO. Hierbei hat die betroffene Person das Recht, problemlos und in angemessenen Zeitabständen Informationen über bereits erhobene Daten zu erhalten, über deren weitere Verwendung unterrichtet zu werden oder diese in Kopie anzufordern.

5.1.5.4 Berichtigung

Die betroffene Person hat jederzeit das Recht, von dem Verantwortlichen die Berichtigung unrichtiger Daten oder die Ergänzung unvollständiger Daten zu verlangen.

5.1.5.5 Datenlöschung / „Recht auf Vergessen“

Des weiteren hat eine Person das Recht – insbesondere, wenn der Zweck, für den die Daten erhoben wurden, erloschen ist - nach Art. 17 DSGVO eine Löschung der sie betreffenden Daten zu verlangen. Von dem Ersuchen auf Löschung der Daten müssen auch weitere Verantwortliche informiert werden, damit die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten durchgeführt wird.

Wird dem Verlangen auf Löschung der Daten nicht entsprochen, ist dies der betroffenen Person gegenüber zu begründen.

Um dem Recht auf Berichtigung oder Löschung nachzukommen ist es sinnvoll, erhobene Daten und bereits vorhandene Daten so aufzuarbeiten und zu clustern, dass Auskunfts – , Berichtigungs - oder Löschungsersuchen der betroffenen Personen ohne sehr großen Aufwand und innerhalb der von der DSGVO vorgegebenen Zeitspanne nachgekommen werden kann.

5.1.5.6 Einschränkung der Verarbeitung

Die betroffene Person hat unter den in Art. 18 DSGVO genannten Voraussetzungen (Bezweifeln der Rechtmäßigkeit der Verarbeitung, der Richtigkeit der Daten usw.) das Recht, vom Verantwortlichen zu verlangen, die Bearbeitung einzuschränken bzw. befristet oder dauerhaft zu unterlassen.

5.1.5.7 Mitteilung über Berichtigung und Löschung

Muss der Verantwortliche eine Berichtigung, Löschung oder Einschränkung der Bearbeitung von personenbezogenen Daten vornehmen, so sind alle weiteren verarbeitenden Stellen der entsprechenden Daten darüber zu informieren. Eine Ausnahme kann hiervon gemacht werden, wenn dies unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist.

5.1.5.8 Automatisierte Entscheidungen, „Dunkelverarbeitung“ und Profiling

Gemäß Art. 22 DSGVO in Verbindung mit den Erwägungsgründen 71 und 72 sollte eine Person von keiner Entscheidung negativ oder beeinträchtigend betroffen sein, wenn diese ausschließlich auf automatisierter Verarbeitung beruht.

Ausnahmen zu diesem Grundsatz in Bezug auf Leistungserbringung aus einem Versicherungsvertrag sind §37 (1) BDSG (neu) zu entnehmen:

- Der beantragten Leistung wird vollumfänglich stattgegeben oder
- Die Entscheidung beruht auf Anwendung verbindlich festgelegter Entgeltregelungen für Heilbehandlungen *und*
    - Es werden Maßnahmen zur Wahrung der Interessen der betroffenen Person getroffen, mindestens die
        - Mitteilung, dass einer Leistung nicht vollumfänglich stattgegeben wurde *und*
        - Information der Person über ihre Rechte *und*
        - Möglichkeit der betroffenen Person, die Entscheidung anzufechten und den eigenen Standpunkt darzulegen *und*
        - Überprüfung der Entscheidung auf Verlangen der betroffenen Person durch manuelles eingreifen in den automatisierten Prozess

Zudem ist Erwägungsgrund 91 zur DSGVO zu entnehmen, dass bei systematischer und eingehender Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten (Gesundheitsdaten) eine Datenschutz – Folgeabschätzung durchgeführt werden sollte.

5.1.5.9 Datenschutzfreundliche Voreinstellungen

Gemäß Art. 25 DSGVO und § 71 BDSG (neu) soll der Datenschutz bereits bei der Gestaltung der Technik (privacy by design) sowie bei der Konfiguration von Anwendungen und Webseiten (privacy by default) berücksichtigt werden. Der Grundgedanke hierbei ist, dass auch Nutzerinnen und Nutzer, die wenig technikaffin oder datenschutzbewusst sind, geschützt werden. Auf Webseiten sollte die Vorbelegung von Checkboxen oder Opt-in Feldern so gewählt werden, dass sie den Benutzern den größtmöglichen Datenschutz bietet oder grundsätzlich unterbleiben, um den Benutzern die Entscheidung über eine Einwilligung o.ä. selbst zu überlassen.

5.1.6 Verantwortlichkeiten

Ein Verantwortlicher, wie z.B. Betreiber eines Internetauftrittes ist nach Art. 5 (2) DSGVO im Sinne der Rechenschaftspflicht dafür verantwortlich, die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten nach Art 5 (1) DSGVO i.V. mit dem Erwägungsgrund 39 nachzuweisen. Diese sind im Einzelnen

- Rechtmäßigkeit,
- Verarbeitung nach Treu und Glauben,
- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität,
- Vertraulichkeit sowie der Nachweis der Einhaltung der

- Technischen und Organisatorischen Maßnahmen.

5.1.7 Stand der Technik

In verschiedenen Artikeln der DSGVO (25,32) wird darauf hingewiesen, dass der Datenschutz nach dem „Stand der Technik“ zu gewährleisten ist. Der „Stand der Technik“ wird hierbei nicht weiter konkretisiert. Durch technische Weiterentwicklungen ist der absolute „Stand der Technik“ variabel, daher sollten Maßnahmen in Bezug auf ihre Wirkungen mit anderen Verfahren verglichen werden, die gewährleisten, dass

- ein Schutzniveau gewahrt wird, welches dem Risiko angemessen ist,
- Datenschutzanforderungen der DSGVO genügt, um die Rechte von betroffenen Personen zu schützen und
- Verantwortliche und Verarbeiter in die Lage versetzt werden, Ihren Verpflichtungen in Bezug auf den Datenschutz nachzukommen.

Auch die regelmäßige Bewertung von Prozessen und Prozessabläufen trägt dazu bei, den „Stand der Technik“ in Bezug auf den Datenschutz zu erreichen.

5.1.8 Auftragsverarbeitung

Verantwortliche, die personenbezogene Daten durch Dritte verarbeiten lassen, haben gem. Art. 28 DSGVO vertraglich festzulegen, dass alle Verpflichtungen zum Schutz personenbezogener auch durch den Auftragnehmer beachtet werden. Die Mindestinhalte eines solchen Vertrages sind u.a.:

- Gegenstand und Dauer des Auftrages (um was für eine Dienstleitung handelt es sich und wie lange soll die Dienstleistung andauern),
- Umfang, Art und Zweck der Dienstleistung (Wozu dient die Dienstleistung, welcher Zielerreichung ist sie dienlich, mit welchen Mitteln wird dies erreicht),
- Art der Daten (welche Daten oder Datenkategorien werden verarbeitet, erhoben oder genutzt),
- Kreis der Betroffenen (Wessen personenbezogene Daten werden verarbeitet, z.B. Mitarbeiter oder Kunden des Auftraggebers),
- konkrete Festlegung der zu treffenden technischen und organisatorischen Maßnahmen,
- Sicherstellung, dass gewährleistet ist, dass personenbezogene Daten berichtigt, gelöscht oder gesperrt werden können,
- Pflichten des Auftragnehmers, insbesondere welche Kontrollen er vorzunehmen hat
- Berechtigung zur Begründung von Unterauftragsverhältnissen,
- Kontrollrechte des Auftraggebers,
- Duldungs- und Mitwirkungspflichten bei diesen Kontrollen,
- Mitteilungspflicht des Auftragnehmers bei Verstößen gegen das BDSG oder den Vertrag,
- Weisungsbefugnisse sowie
- Verfahrensweise mit Datenträgern und Unterlagen bei Ende der Dienstleistung

5.1.9 Backup- und Cloudlösungen

Sofern einer Backup-oder Cloudlösung eines externen Anbieters genutzt werden soll, sind die Regelungen des Art. 28 DSGVO bezüglich der Auftragsdatenverarbeitung zu beachten. Eine weitere Anforderung an den Cloudanbieter ist die Beachtung der Regelungen der DSGVO. Als ein Beleg hierfür kann eine Zertifizierung gemäß Artikel 42, 43 DSGVO dienen.

5.1.10 Löschstrategien

Gemäß Art. 17 DSGVO hat eine betroffene Person ein Recht auf die Löschung aller sie betreffenden Daten. Das Recht auf Datenlöschung kann durch die Verantwortlichen nur dann mit vertretbarem Aufwand umgesetzt werden, wenn Datenspeicherungs- und Löschstrategien dies unterstützen.
Beispielsweise sind Mitarbeiter- und Kundendaten nach dem Gebot der getrennten Datenhaltung ggf. unterschiedlich gespeichert oder sollen nach verschiedenen Fristen gelöscht werden. Sofern der Zweck der Datenerhebung beendet ist, könnte es erforderlich sein diese verschiedenen Datentypen zu finden und zu löschen.

Darüber hinaus besteht die Verpflichtung, alle weiteren für die Datenverarbeitung Verantwortlichen darüber informieren, dass alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen sind. Im Rahmen der Speicherung personenbezogener Daten beim Betrieb einer Webseite müssten alle Institutionen, die von dieser Seite personenbezogene Daten beziehen (auch Werbetreibende, Anbieter von Webseitenstatistiken oder sozialen Medien usw.) darauf hingewiesen werden, diese zu löschen. Hierfür ist ein geregelter Prozess zu etablieren.

5.1.11 Meldung und Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten

Gemäß Artikel 33 und 34 DSGVO bestehen Meldepflichten gegenüber den Aufsichtsbehörden sowie den betroffenen Personen, sobald der Schutz personenbezogener Daten bekannt geworden ist. Die Meldung an die Aufsichtsbehörden hat innerhalb von 72 Stunden zu erfolgen, die Meldung an die betroffenen Personen muss unverzüglich nach Bekanntwerden erfolgen. Eine Ausnahme kann gemacht werden, wenn die Schutzverletzung kein Risiko (bei Meldungen an die Aufsichtsbehörde) oder kein hohes Risiko (bei Meldungen an die betroffene Person) für die persönlichen Rechte und Freiheiten natürlicher Personen darstellt. Wird den Betreibern einer Webseite bekannt, dass diese Ziel eines Angriffes wurde und wird diese Webseite genutzt, z.B. um Daten einer hohen Schutzkategorie zu erfassen (Sozialdaten), so ist von einem hohen Risiko für die betroffenen Personen auszugehen und in der Folge sind diese zu benachrichtigen. Dieses gilt auch für Datenverarbeitung im Auftrag.

5.1.12 Datenschutzfolgeabschätzung

Gemäß Art. 35 DSGVO ist bei einer Verarbeitung, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, durch Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Bei Verfahren, die der Verarbeitung besonderer personenbezogener Daten (Sozialdaten) dienen, ist davon auszugehen, dass eine Datenschutz-Folgeabschätzung durchzuführen ist. Diese ist alle 3 Jahre zu wiederholen.
Die Datenschutzfolgeabschätzung muss mindestens folgende Inhalte enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.

Zur Checkliste

5.2 Datenschutzerklärung

Die Checkliste in der Anlage 4 kann teilweise von der Revision ausgefüllt werden, einige Fragen erfordern eine Beantwortung des Webseitenbetreibers bzw. der technischen Verantwortlichen. Diese sind gesondert aufgeführt.

Grundsätzlich ist mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO), (Artikel 25), durch die Gestaltung der Technik, datenschutzfreundliche Voreinstellungen und organisatorische Maßnahmen dafür Sorge zu tragen, dass Datenschutzgrundsätze wie etwa Datenminimierung wirksam ungesetzt werden, um den Anforderungen der DSGVO zu genügen und Rechte der Nutzer zu schützen.

Die Pflicht zu einer Datenschutzerklärung ergibt sich aus dem § 13 Abs. 1 TMG. Ab 05./2018 gelten die Vorgaben der DSGVO (Datenschutzgrundverordnung). Die Anbieterinnen und Anbieter von Telediensten haben die Nutzer zum Anfang des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten in allgemein verständlicher Form zu unterweisen. Dies betrifft somit jede Betreiberin bzw. jeden Betreiber einer Website, da nach allgemeiner Auffassung die zur Kommunikation im Internet notwendige IP-Adresse bereits ein personenbezogenes Datum darstellt. Der Inhalt der Unterweisung muss dabei für die Nutzerinnen und Nutzer jederzeit abrufbar sein und neben den personenbezogenen Daten auch Zweck und Dauer der Speicherung erläutern.

Ob und welche Daten beim Besuch einer Website erhoben werden, ist sehr unterschiedlich. In wie weit IP-Adressen für systeminterne Logdateien bzw. zur Reichweitenanalyse verwendet werden, können die Betreibenden beim zuständigen Provider erfahren. Benutzt man zum Betrieb der Website ein Content Management System (CMS) , werden häufig Cookies, E-Mail-Adressen, (Benutzer-)Namen u.ä. personenbezogene Daten ebenfalls abgespeichert. Diese Informationen erhalten die Betreibenden aus dem Datenblatt der jeweils benutzen Software. Stellt man zur Kontaktaufnahme ein E-Mail-Formular bereit, ist die Empfängerin bzw. der Empfänger der E-Mail klar zu benennen, sowie Zweck und Dauer der Speicherung der E-Mail. Zur Reichweitenmessung der Website eingesetzte externe Tools, wie z. B. „Google Analytics“, verarbeiten ebenfalls personenbezogene Daten, wie etwa IP-Adressen oder Browser Fingerprints (charakteristische Daten zum verwendeten Browser).

Webseitenbetreibende sollten nach dem Urteil des OLG Hamburg vom 27.06.2013 – Az. 3 U 26/12 die Datenschutzerklärung neben dem Impressum als eigenen Punkt im Header oder Footer von jeder Seite der Webseite erreichbar vorsehen.

Aus den genannten Beispielen wird ersichtlich, dass man i. d. R. davon ausgehen kann, dass Betreiber einer Website personenbezogene Daten speichern, verarbeiten und teilweise übertragen. Diese Informationsströme sind den Nutzern nicht in jedem Falle klar ersichtlich. Durch das Recht auf informationelle Selbstbestimmung haben die Webseitenbesucherinnen und –besucher aber das Recht zu erfahren, welche Daten wohin übertragen werden. Dieses Recht auf Auskunft können die Nutzerinnen und Nutzer bei

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

den Betreibenden der Website gemäß § 34 Bundesdatenschutzgesetz (BDSG) und ab 05/2018 auf Grundlage der DSGVO, Art. 15 ff., geltend machen. Nach Inkrafttreten der DSGVO sind die Rechte der Nutzerinnen und Nutzer dahingehend gestärkt, dass diese z.B. auch Informationen über
„das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“
von der Stelle, die personenbezogene Daten verarbeitet, anfordern kann. Dies hat zufolge, das den Nutzerinnen und Nutzern, deren personenbezogene Daten verarbeitet werden, ggf. auf Anforderung über Regelwerke u.a. Auskunft gegeben werden muss.

Eine Auflistung der Grundsätze des Datenschutzrechts und deren Umsetzung in den Datenschutzgesetzen des Bundes und der Länder ist auf der folgenden Seite zu finden. Ab dem Zeitpunkt des Inkrafttretens der DSGVO werden eine Vielzahl von einzelgesetzlichen Regelungen durch die Normen der DSGVO ersetzt bzw. ergänzt.

Um Vergleiche zwischen den Regelungen der DSGVO und den alten Regelungen anstellen zu können, werden die alten Regelungen in diesem Leitfaden noch einige Zeit beibehalten, sind aber zum Teil ab dem 25.05.2018 obsolet.

Synopse: Vorschriften des Bundes- und der Landesdatenschutzgesetze

Inhalte	BDSG	BW	Bayern	Bln	Bbg	Bremen	Hmb	Hessen
Verbot mit Erlaubnisvorbehalt	§ 4 I	§ 4 I	Art. 15 I	§ 6 I	§ 4 I	§ 3 I	§ 5 I	§ 7 I
Grundsatz der Zweckbindung	§§ 4a I, 14 II	§§ 4 II, 14	Art. 15 II, 16 III, 17 I, 22	§§ 6 III, 11	§§ 4 II, 13	§§ 3 III, 12	§§ 5 II, 13	§§ 7 II, 11, 13
Direkterhebungsgrundsatz	§ 4 II	§§ 4 II, 13 II, 14 I	Art. 16 II	§ 10 I	§ 12 II	§ 1o II	§ 12 II	§ 12 I
Grundsatz der Richtigkeit	§ 35 I	§ 22	Art. 11	§ 17 I	§ 19 I	§ 22 I	§ 19 I	§ 19 I
Transparenz	§ 34	§ 21	Art. 10	§§ 5 II Nr. 6, 16	§ 10 II Nr. 6, 18	§ 21	§ 19 I	§ 18
Verhältnismäßigkeit	§§ 13 ff	§§ 13 ff	Art. 16 ff	§§ 9 ff	§§ 12 ff	§§ 10 ff	§§ 12 ff	§§ 11 ff
Datenvermeidung / Datensparsamkeit	§ 3a	§ 9 I		§ 5 a	§ 7 I S. 2	§ 7 I	§ 5 IV	§ 10 II
Begriffsbestimmungen	§ 3	§ 3	Art. 4	§ 4	§ 3	§ 2	§ 4	§ 2
Besondere Arten von personenbezogenen Daten	§ 3 IX	§ 33	Art. 15 VII	§ 6 a	§ 4a	§§ 2 VI; 3 II	§ 5 I S. 2	§ 7 IV
Technisch-organisatorische Maßnahmen	§ 9 inkl. Anlage	§ 9	Art. 7	§ 5	§ 10	§ 7	§ 8	§ 10
Vorabkontrolle	§ 4d V, VI	§ 12	Art. 26	§ 5 III	§ 10a	§ 7 II	§ 8 IV	§§ 7 VI, 5 V
Verfahrensverzeichnis	§ 4e	§ 11	Art. 27	§§ 19 II, 19a	§ 8	§ 8	§ 9	§ 6
Auftragsdatenverarbeitung	§ 11	§ 7	Art. 6	§ 3	§ 11	§ 9	§ 3	§ 4
Zulässigkeit der Datenverarbeitung	§ 4 I	§ 4 I	Art. 15	§ 6 I	§ 4 I	§ 3 I	§ 5 I	§ 7 I
Rechtsgrundlagen der Datenverarbeitung	§§ 12 - 18	§§ 13 – 20 a	Art. 16 - 21	§§ 9 - 14	§§ 12 - 17	§§ 10 – 20b	§§ 12 - 17	§§ 11 - 17
Behördl. Datenschutzbeauftragter	§ 4f, g	§ 10	Art. 25	§ 19 a	§ 7a	§ 7a	§ 10a	§ 5
Rechte der Betroffenen	§§ 6, 19 - 21	§§ 5, 21 - 25	Art. 9 - 14	§§ 7, 16 - 18	§§ 5, 18 - 21	§§ 4, 21 - 23	§§ 6, 18 - 20	§§ 8, 18 - 20
Beschäftigtendatenschutz	§ 32	§ 36			§ 29	§ 20	§ 28	§ 34
Landesbeauftragter für Datenschutz	§§ 22 - 26	§§ 26 – 32 a	Art. 29 - 32	§§ 21 - 29	§§ 22 - 27	§§ 24 - 35	§§ 21 - 26	§§ 21 - 31
Bußgeld - / Strafvorschriften	§§ 43 - 44	§§ 40, 41	Art. 37	§ 32	§ 38	§§ 37 - 38	§§ 32 - 33	§§ 40, 41
Verbundverfahren					§ 9	§ 14a	§ 11a	§ 15
Automatisierte Abrufverfahren	§ 10	§ 8	Art. 8	§ 15	§ 9	§ 14	§ 11	
Besonderer Datenschutz	§§ 39 – 42a	§§ 33 - 38	Art. 21a - 23	§§ 30 – 31 c	§§ 28 – 33d	§§ 19 – 20b	§§ 27 - 31	§§ 32 - 37
Personalaktenrecht	§§ 106 - 115 BBG	§§ 83 - 88 LBG	Art. 101 – 111 BayBG	§§ 84 - 91 LBG	§§ 94 – 101 LBG	§§ 85 - 92 BremBG	§§ 85 - 92 HmbBG	§§ 86 - 93 HBG

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Synopse: Vorschriften des Bundes- und der Landesdatenschutzgesetzte

Inhalte	MV	Nds	NRW	RP	Saar	Sachs	LSA	SH	Thür
Verbot mit Erlaubnisvorbehalt	§ 7 I	§ 4 I	§ 4 I	§ 5 I	§ 4 I	§ 4 I	§ 4 I	§ 11 I	§ 4 I
Grundsatz der Zweckbindung	§§ 9 III, 10 II	§§ 9 II, 10 I	§§ 4 I, 13	§§ 5 II, 13 I Nr. 2	§§ 4 I, 13	§§ 4 III, 13	§§ 4 II, 10	§ 13	§§ 4 III, 20
Direkterhebungsgrundsatz	§ 9 II	§ 9 I S. 2	§ 12 I S. 3	§ 12 II	§ 12 I S. 2	§ 12 II	§ 9 II	§ 13 I	§ 19 II
Grundsatz der Richtigkeit	§ 25 I	§ 17 I	§ 19 I	§ 19 I	§ 21 I	§ 19 I	§ 16 I	§ 28 I	§ 14
Transparenz	§§ 21 II Nr. 6, 24	§ 16 I	§ 10 II Nr. 6	§ 18	§ 22	§ 9 II Nr. 6, 18	§ 5 II Nr. 6, 15	§§ 5 I Nr. 4; 27	§§ 9 II Nr. 6, 13
Verhältnismäßigkeit	§§ 9 ff	§§ 9 ff	§§ 12 ff	§§ 12 ff	§§ 12 ff	§§ 12 ff	§§ 9 ff	§§ 13 ff	§§ 19 ff
Datensparsamkeit	§ 5 I	§ 7 IV	§ 4 II	§ 1 III	§ 4 IV	§ 9 I	§ 1 II	§ 4 I	§ 1 II
Begriffsbestimmungen	§ 3	§ 3	§ 3	§ 3	§ 3	§ 3	§ 2	§ 2	§ 3
Besondere Arten von personenbezogenen Daten	§ 7 II	§ 4 II	§ 4 III	§§ 3 IX, 5 IV	§ 4 II	§ 4 II	§§ 2 I, 26	§ 11 III	§ 4 V
Technisch-organisatorische Maßnahmen	§ 21	§ 7	§ 10	§ 9	§ 11	§ 9	§ 6	§§ 5, 6	§ 9
Vorabkontrolle	§ 19	§ 8 a III	§ 10 III	§§ 9 V, 11 III	§ 11 I	§ 10 IV	§ 14 II	§ 9	§ 10a II, 34 II
Verfahrensverzeichnis	§ 18	§ 8	§ 8	§ 10 III	§ 9	§ 10 I	§ 14 III	§ 7	§ 10
Auftragsdatenverarbeitung	§ 4	§ 6	§ 11	§ 4	§ 5	§ 7	§ 8	§ 17	§ 8
Zulässigkeit der Datenverarbeitung	§ 7 I	§ 4 I	§ 4 I	§ 5 I	§ 4 I	§ 4 I	§ 4 I	§ 11 I	§ 4 I
Rechtsgrundlagen der Datenverarbeitung	§§ 9 - 17	§§ 9 - 15	§§ 12 - 17	§§ 12 – 17	§§ 12 - 18	§§ 12 - 17	§§ 9 - 13	§§ 13 - 16	§§ 19 – 25a
Behördl. Datenschutzbeauftragter	§ 20	§ 8 a	§ 32 a	§ 11	§ 8	§ 11	§ 14a	§ 10	§ 10 a
Rechte der Betroffenen	§§ 24 - 28	§§ 16 - 20	§§ 5, 18 - 20	§§ 6, 18 - 21	§§ 19 - 24	§§ 5, 18 - 22	§§ 15 - 19	§§ 26 - 31	§§ 5, 11 - 18
Beschäftigtendatenschutz	§ 35	§ 24	§ 29	§ 31	§ 31	§ 37	§ 28	§ 23	§ 33
Landesbeauftragter für Datenschutz	§§ 29 – 33b	§§ 21 - 23	§§ 21 - 27	§§ 22 - 29	§§ 25 - 29	§§ 25 - 31	§§ 20 - 24	§§ 32 - 43	§§ 35 - 40
Bußgeld - / Strafvorschriften	§§ 42 - 43	§§ 28 - 29	§§ 33 - 34	§ 37	§§ 35 - 36	§§ 38 - 39	§§ 31 – 31a	§§ 44 - 45	§ 43
Verbundverfahren	§ 17		§ 4 a					§ 8	§ 7 a
Automatisierte Abrufverfahren	§ 17	§ 12	§ 9	§ 7	§ 10	§ 8	§ 7	§ 8	§ 7
Besonderer Datenschutz	§§ 34 - 39	§§ 24 - 27	§§ 28 - 32	§§ 30 - 35	§§ 30 - 34	§§ 32 - 37	§§ 25 – 30a	§§ 18 - 24	§§ 25a, 26 ff
Personalaktenrecht	§§ 84 - 91 LBG-M-V	§§ 88 - 95 NBG	§§ 84 - 91 LBG-NRW	§§ 87 - 96 LBG-Rh.-Pf.	§§ 95 - 102 SBG	§§ 117 – 124 Sächs BG	§§ 84 - 91 LBG- LSA	§§ 85 - 92 LBG	§§ 89 - 96 ThürBG

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

5.2.1 Facebook-Button

Nach der Rechtsprechung zum Stand der Erstellung dieses Prüfleitfadens wird davon ausgegangen, dass das Sammeln von Daten ohne Hinweis darauf, dass Daten erhoben werden, welche Daten erhoben werden und an wen diese Daten zu welchem Zweck übermittelt werden, unzulässig ist. (Siehe auch Urteil des EUGH Urteil in der Rechtssache C-362/14 („Safe-Harbor-Regelung“) in Verbindung mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) Diese Rechtsprechung wird ab 05./2018 in der DSGVO umgesetzt.

Dies stellt die Webseitenbetreiber aber vor ein nahezu unlösbares Problem, auch wenn sie an die Aufklärung grundsätzlich denken: Im Zweifel wissen die Webseitenbetreiber – gerade im Falle von Facebook – selbst nicht genau, wann der „Like-Button“ Daten sammelt, welche Daten er sammelt und an wen diese Daten übermittelt werden.

5.2.2 Beispiele zu Datenschutzproblemen im Internet

Wer viel im Netz unterwegs ist, hinterlässt Spuren, die für die Wirtschaft extrem interessant sind. Auf das Sammeln dieser Informationen haben sich Datenhändler spezialisiert, die für ihre Kundinnen und Kunden (die Betreiber von Webseiten) noch einen besonderen Service anbieten: Sie ordnen die Konsumenten verschiedenen wirtschaftlichen Kategorien zu. So können Unternehmen zum Beispiel ihre Werbung gezielt verbreiten.

Fall 1: Reisebuchung: Eine US-Amerikanerin will über den Veranstalter „Airbnb“ ein Zimmer in Bremen buchen, doch die Buchung klappt nicht. Als die Frau bei der Hotline um Hilfe bittet, fragt man sie, wie viele Facebook-Freunde sie hat. Sie antwortet: 50. Zu wenig. Denn Nutzer mit unter 100 Facebook-Freunden sind für die Firma nicht die geeignete Zielgruppe.

Fall 2: Einkaufen mit Kundenkarte: Von der Supermarktkette, bei der sie regelmäßig shoppt, werden einer Minderjährigen Rabattcoupons für Babykleidung und Schnuller per Post zugeschickt. Der Vater hakt nach, wie der Markt dazu komme. Es stellt sich heraus: Seine Tochter ist tatsächlich schwanger. Erkennen konnte der Markt das an ihrem Einkaufsverhalten, das über ihre Kundenkarte dokumentiert wurde.

Fall 3: Dynamische Preise: Ein US-Online-Reiseportal hat einen Monat lang bewusst zwischen Apple- und Nicht-Apple-Nutzerinnen und Nutzern unterschieden. Wer mit einem Apple-Gerät auf die Seite kam, erhielt die Reiseangebote mit einem höheren Preis angezeigt als Kundinnen und Kunden mit anderen Endgeräten. Das Ergebnis: Viele der Apple-Nutzenden waren bereit, den höheren Preis zu zahlen.

zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

6 DATENSICHERHEIT (ANBIETER)

Das Thema Datensicherheit bzw. sichere Internetseiten hat zwei unterschiedliche Aspekte: Einerseits muss die Internetseite mit ihren Inhalten sowie den dahinter liegenden Anwendungen und Datenbanken vor Sicherheitsrisiken bewahrt werden. Zum anderen sind die Besucherinnen und Besucher der Webseite vor Gefahren zu schützen und ihre Daten vor dem Zugriff Dritter zu sichern. Da für beide Themen umfangreiche Maßnahmen zu beachten sind, werden sie in dieser Prüfhilfe separat behandelt. Auch die Checklisten (Anlage 5, Absicherung der Webseiten und Anlage 6, Schutz der Webseitenbesucher) sind thematisch voneinander getrennt, obwohl einige Überschneidungen nicht zu vermeiden sind. Die Fragen in der Checkliste zum Thema Datensicherheit sind komplett von den Betreibenden der Webseite zu beantworten.

Das umfangreiche Thema Sicherheit von Webseiten ist sehr von aktuellen Entwicklungen geprägt, so dass es im Rahmen dieses Prüfleitfadens nie vollständig behandelt werden kann. Im Prüfleitfaden und auch in den Checklisten können nur Anregungen für Prüfansätze und Risikobewertungen gegeben werden. Im Rahmen einer Prüfung werden immer wieder Themen behandelt werden, die in diesen Prüfleitfaden noch nicht oder nicht in vollem Umfang eingeflossen sind.

Hintergrundinformationen, auch technischer Art, sind im „Technischen Handbuch Internet“ zu finden, Fachbegriffe sind dort im Bereich „Glossar“ erläutert.

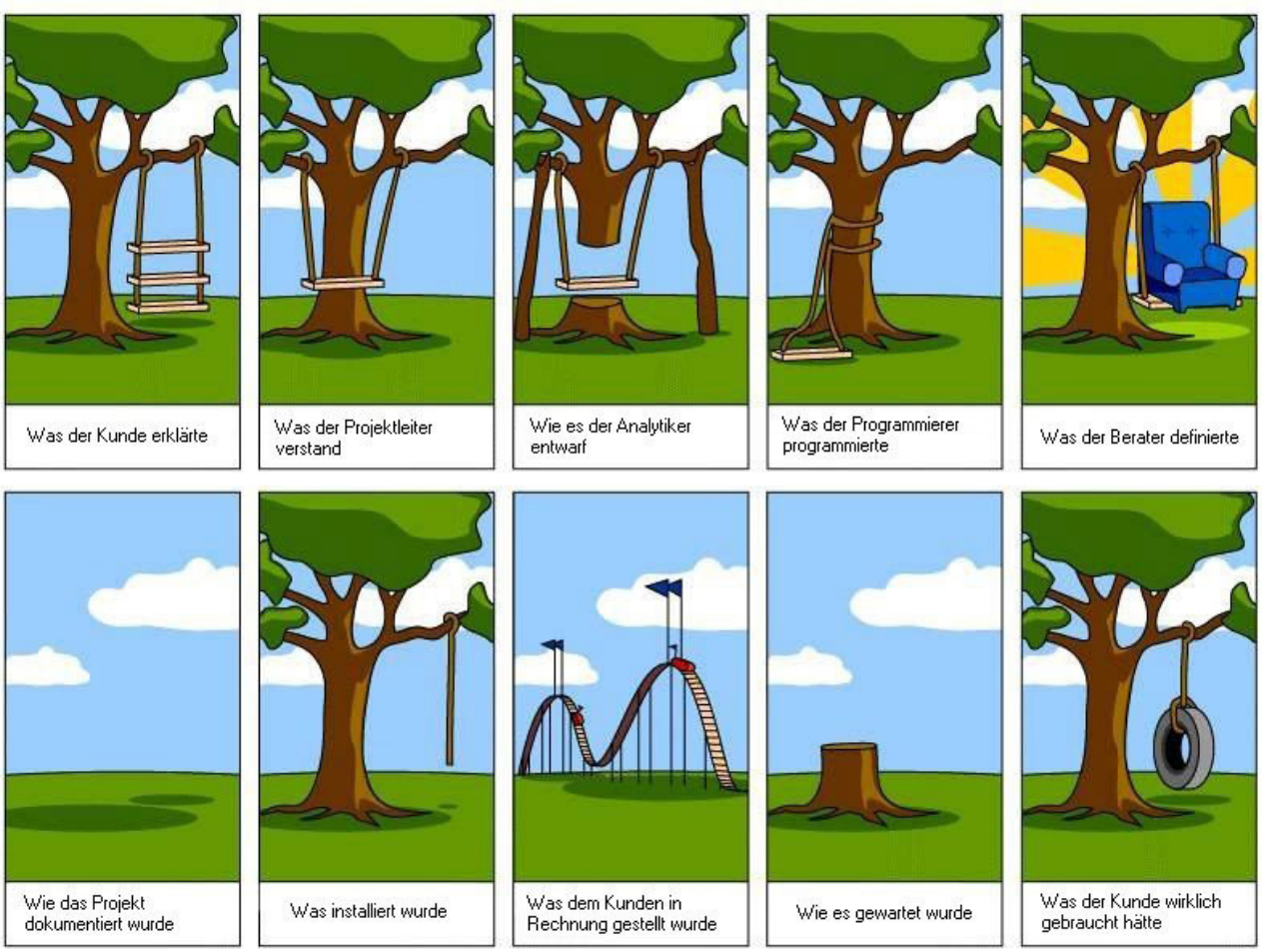
6.1 Betreiben einer sicheren Webseite

6.1.1 Softwareentwicklung

Eine sichere Internetseite kann nur dann gestaltet werden, wenn die Entwicklung und der Betrieb der einzelnen Komponenten in einem gesicherten Verfahren abläuft, mit dem bereits bekannte Fehlerquellen weitgehend vermieden werden können.
Eine geregelte Softwareentwicklung gliedert sich in folgende Teilschritte:

- Planung (Lastenheft / Definition der Anforderungen)
- Analyse (Welche Prozesse entstehen aus den Anforderungen)
- Entwurf (Wie muss die Software entwickelt werden, um die Anforderungen zu erfüllen?)
- Programmierung (Umsetzung der Prozesse in die Software)
- Testverfahren (Ist die Software auf dem System lauffähig? / Werden die Anforderungen erfüllt? / Wurde entwickelt, was der Kunde erwartet?)
- Dokumentation (Beschreibung der Software / der Bedienung / der Systemumgebung usw.)
- Qualitätssicherung (Sind auch die nicht-funktionalen Anforderungen erfüllt? /z.B. Ergonomie, Rechtschreibung, Dokumentation)
- Konfigurationsmanagement (Versionsverwaltung, Update-, Änderungsmanagement)

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.



Diese Bilderreihe erklärt besser als viele Worte, welche Punkte bei der Softwareentwicklung berücksichtigt werden müssen und wo die häufigsten Fahler gemacht werden.

6.1.2 Auswahl vertrauenswürdiger Anbieter

Besonders für Webseitenbetreibende, die keine eigene IT-Abteilung haben, ist es ratsam, ihre Webseitenerstellung an professionelle Dienstleister auszulagern. Mit Erfahrungen im Bereich der IT-Sicherheit sind diese in der Lage, beispielsweise einen geschützten Bereich innerhalb der Internetseite aufzubauen.

Vor der Entscheidung für eine Anbieterin oder einen Anbieter sollten dessen Sicherheitsvorkehrungen geprüft werden. Informationen über die Art der Dokumentation der IT-Infrastruktur und der Versionsverwaltung, die dort eingesetzt werden, sind vor der Beauftragung einzuholen. Diese sind Basis für eine Absicherung des Systems. In einem Notfall besteht dadurch die Gelegenheit, schnell zum letzten lauffähigen und integren Stand zurückzuspringen. Insbesondere wenn Cyberkriminelle den Webauftritt kompromittiert haben, ist es außerordentlich wichtig, mit Hilfe der Versionsverwaltung nachvollziehen zu können, welcher Stand integer ist und diesen wiederherzustellen. Unter die Dokumentation fällt die Konfiguration aller Systemkomponenten, die Art der Vernetzung und die wichtigsten Kontaktdaten von Dienstleistern. Auch die Bemessung des Reifegrades der Software bzw. der Softwareentwicklungsprozesse (hierzu gehören

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

z.B. Existenz und Einhaltung von Programmierrichtlinien oder Testverfahren) ist ein wichtiges Entscheidungsmerkmal.

6.1.3 Sicherheitskonzept für den Betrieb einer Webseite

Bereits bevor es zur Realisierung der Webseiten durch eine Dienstleisterin bzw. einen Dienstleister kommt, sollte sichergestellt sein, dass die auftraggeberseitigen Sicherheitsansprüche voll erfüllt sind. Auch für den Betrieb einer Webseite ist ein Sicherheits- und Benutzerkonzept zu empfehlen. Weiterhin ist vertraglich festzuhalten, dass Sicherheitsupdates für Web-Dienste und Module zeitnah eingespielt werden. Hierunter fallen sowohl Systemupdates wie zum Beispiel für den Webserver als auch Sicherheitsupdates für das Content Management System (CMS) und für Erweiterungsmodule. Weiterhin sollte geregelt sein, dass die Logfiles des Servers regelmäßig überprüft werden, damit Unregelmäßigkeiten, die auf Angriffsversuche hinweisen könnten, frühzeitig erkannt werden.

Wenn sensible (personenbezogene oder Sozial-) Daten auf der Website eingegeben werden, ist für eine sichere Datenübertragung und -speicherung mittels geeigneter Verschlüsselungstechniken zu sorgen. Für die sichere Übertragung von Daten eignet sich das Verfahren Secure Sockets Layer, kurz SSL bzw. die Nachfolgeversion TLS (Transport Layer Security) (Stand 06/2015). Bei der Datenspeicherung ist sicherzustellen, dass die Benutzerpasswörter ausschließlich nach aktuellen Standards als sogenannte Hashsummen in der Datenbank hinterlegt werden und niemals im Klartext.

Besonders Eingabemöglichkeiten wie Formulare oder Freitexteingaben sollten auf sicherheitskritische Funktionalitäten geprüft werden. Sind Formularfelder nicht sicher programmiert, kann durch Angriffsmethoden, wie sogenannte SQL-Injections oder Cross-Site-Scripting, das Einschleusen von schädlichem Code möglich sein.

Wenn alle Maßnahmen nicht verhindert haben dass die Webseite gehackt wurde, sollte das Sicherheitskonzept Maßnahmen enthalten wie ggf. forensische Beweise gesichert werden und – relevanter für die Betreibenden der Webseite – wie die Seite so schnell wie möglich wieder in Betrieb gehen kann.

6.1.3.1.1 Benutzernamen

Bei der Anmeldung für den Benutzerbereich auf einer Webseite können die Benutzerinnen und Benutzer ihren Anmeldenamen in der Regel frei wählen. Auf Seiten der Webseitenbetreibenden sind folgende Sicherheitsaspekte zu beachten:

- Benutzernamen dürfen nicht doppelt vergeben werden

- Die Anmeldedaten (Benutzername und Kennwort) sind auf dem Anmeldeserver in gesicherten Bereichen verschlüsselt bzw. als Hashwert abzulegen
- Die Anmeldedaten dürfen nicht ohne Wissen der Nutzerinnen und Nutzer als Cookie lokal auf dem Rechner gespeichert werden

6.1.3.1.2 Kennwörter

Zum Schutz vor unberechtigten Zugriffen wurden durch das BSI folgende Kennwortrichtlinien empfohlen:

Maximales Kennwortalter	90 Tage
Minimales Kennwortalter	1 Tag
Minimale Kennwortlänge	8 Zeichen
Kennwortchronik	6 Kennwörter
Kontosperrungsschwelle	3 Versuche
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten
Kontosperrdauer	60 Minuten

Als Kennwortkomplexität wird vom BSI die Verwendung von Groß- und Kleinschreibung und Sonderzeichen empfohlen.

Diese Kennwortrichtlinien sind als Anregung zu betrachten und regelmäßig auf Sinnhaftigkeit im eigenen System zu überprüfen. Insbesondere durch die Steigerung der Leistungsfähigkeit der Hardware und die Veröffentlichung von Sicherheitslücken ist eine regelmäßige Neubewertung der Kennwortrichtlinien erforderlich. Beispielsweise kann die minimale Kennwortlänge von 8 Zeichen nicht mehr zeitgemäß erscheinen, um einen Angriff auf eine Anwendung zu verhindern. Bereits mit einem handelsüblichen Rechnersystem kann solch ein Kennwortschutz durch eine „Brute-Force-Attacke“ (ausprobieren von möglichen Kennwortkombinationen) je nach Komplexität des genutzten Kennwortes in kurzer Zeit überwunden werden.

Maximale Rechenzeit eines Brute-Force-Angriffs bei einer Milliarde Schlüsseln pro Sekunde

Zahl und Art verwendeter Zeichen (Zeichenraum)	Passwortlänge 4 Zeichen	6 Zeichen	8 Zeichen	10 Zeichen	12 Zeichen
10 [0-9]	unter 1 ms	unter 1 ms	100 ms	10 Sek.	17 Min.
26 [a-z]	unter 1 Sek.	unter 1 Sek.	4 Min.	2 Tage	3 Jahre
52 [a-z + A-Z]	unter 1 Sek.	20 Sek.	15 Stunden	5 Jahre	12.400 Jahre
62 [a-z + A-Z + 0-9]	unter 1 Sek.	58 Sek.	3 Tage	27 Jahre	102.000 Jahre
96 (alles plus Sonderzeichen)	unter 1 Sek.	13 Min.	84 Tage	2108 Jahre	19 Mio. Jahre

Daten: Wikipedia
Legende: sehr sicher | einigermaßen sicher | nicht sicher

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Abhilfe schaffen Komplexitätsanforderungen an Kennwörter, die einen größtmöglichen Zugangsschutz gewährleisten. Unterstützend hierzu sollte auch ein systemweites Monitoring genutzt werden, dass Auskunft über den Systemzustand sowie Auffälligkeiten (wie mehrfache falsche Kennworteingabe usw.) gibt.

Folgende Kennwortrichtlinien werden vorgeschlagen:

- Kennwortlänge mindestens 10 Zeichen
- Kennwortkomplexität
    - Großbuchstaben +
    - Kleinbuchstaben +
    - Ziffern +
    - Sonderzeichen +
    - Mindestens 3 der 4 Zeichenarten müssen im individuellen Kennwort verwendet werden
- Sperrzeit nach Fehleingaben des Kennwortes exponentiell ansteigend
    - z.B. (in Sekunden): 3,5,10,15,20,30,45,60,120,300,900,Kontosperre
- Kontorücksetzung nur nach sicherer Identifikation des Nutzers durch die IT-Abteilung
- Verwendung der letzten 10 Kennwörter nicht erlaubt
- Minimales Kennwortalter nicht unter 12 Stunden

Die Forderung nach komplexen Kennwörtern schafft allerdings ein weiteres Problem. Wissenschaftlichen Auswertungen zufolge sind die Nutzerinnen und Nutzer mit der Vielzahl von Kennwörtern und Geheimzahlen zunehmend überfordert. Wenn Kennwortänderungen erzwungen werden, versuchen sie häufig, das alte Kennwort nur leicht abzuwandeln oder ein wenig sicheres - aber leicht zu merkendes - Kennwort zu benutzen.

Ein Lösungsweg ist, die Methode des erzwungenen, regelmäßigen Kennwortwechsels auf den Prüfstand zu stellen. In einer sicheren Systemumgebung kann ein regelmäßiger Kennwortwechsel nicht zwingend erforderlich sein, da dieser nur die Nutzerinnen und Nutzer belastet und keine zusätzliche Sicherheit schafft. Sinnvoller wäre es, einen erzwungenen Kennwortwechsel anlassbezogen, z.B. nach einem Angriff auf ein System oder bekanntwerden einer Sicherheitslücke durchzuführen.

In der Vergangenheit sind bei verschiedenen Hackerangriffen mehrfach Datenbanken mit Millionen Log-In-Daten erbeutet worden. Hierdurch ist eine sehr große Datenbasis genutzter Kennwörter entstanden. Hier als Beispiel die Rangliste der beliebtesten Kennwörter in Deutschland (2017):

1. 123456	2. 123456789	3. 1234	4. 12345	5. 12345678
6. hallo	7. passwort	8. 1234567	9. 111111	10. hallo123

Mit den erbeuteten Kennwort-Datenbanken lassen sich problemlos und in kurzer Zeit erfolgversprechende Angriffe auf kennwortgeschützte Systeme durchführen, da eine hohe Wahrscheinlichkeit besteht, dass Benutzer ihre Kennwörter für mehrere Systeme genutzt haben. Zur Erhöhung der Systemsicherheit könnten die von den Benutzern vergebenen Kennwörter mit den o.a. Kennwortdatenbanken abgeglichen und ggf. abgelehnt werden.

Um unbefugten Zugang zu den Systemen zu verhindern, kommt weiterhin der Schulung und Information der Mitarbeiterinnen und Mitarbeiter besondere Bedeutung zu.

- Für jeden Dienst sollten Benutzerinnen und Benutzer ein eigenes Kennwort verwenden.
- Am sichersten sind Kennwörter, die aus einer Zufallskombination aller zur Verfügung stehenden Zeichenarten bestehen.
- Nicht nur die Zusammensetzung, auch die Länge des Kennwortes ist wichtig, zur Zeit erscheint eine Kennwortlänge von 10-12 Zeichen zweckmäßig.
- Wenn komplexe Kennwörter genutzt werden, kann ein regelmäßiger, erzwungener Kennwortwechsel die Systemsicherheit nicht positiv beeinflussen.
- Bei der Nutzung verschiedener, passwortgeschützter Dienste könnte eine Passwort-Manager-Software eine zweckmäßige und sichere Alternative darstellen.

6.1.3.1.3 Weitere Sicherheitsvorkehrungen

Notfallplanungen:

Für den Webserver ist durch den Anbieterin bzw. den Anbieter ein Notfallkonzept vorzulegen, in welchem die Planungen für den Falles eines Ausfalls der Infrastruktur sowie die Maßnahmen zur Inbetriebnahme beschrieben sind.

- Durch einen Systemausfall kann es zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für den Webserver zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte. Hierin sollte nicht nur der Webserver selbst, sondern auch das Gesamtsystem, innerhalb dessen der Webserver eingesetzt wird, berücksichtigt werden. Dazu gehören unter Umständen Datenbanken, Applikationsserver oder Proxy-Installationen zur Lastverteilung.
- Bestehen besondere Anforderungen an die Verfügbarkeit des Webservers, so sollten benötigte Komponenten redundant ausgelegt werden. Beispielsweise kann der Webserver selbst in manchen Anwendungen durch die Verwendung eines gemeinsamen, externen Speichersystems redundant ausgelegt werden.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

- Zum Betrieb des Webservers im Internet ist eine funktionierende Internet-Anbindung Voraussetzung. Bei bestimmten Konfigurationen ist auch ein korrekt funktionierender DNS-Server nötig. Ein Ausfall dieser Komponenten muss daher ebenfalls in Betracht gezogen werden.
- Wird SSL auf dem Webserver eingesetzt, so muss beim Wiederanlauf des Systems auch der private Schlüssel des SSL-Zertifikates zugreifbar sein. Da dieser durch ein Passwort sicher geschützt sein sollte, muss dieses zugreifbar hinterlegt sein, damit es für den Wiederanlauf verfügbar ist.
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems und der Einzelkomponenten in der richtigen Reihenfolge gewährleistet.

6.1.4 Verhindern der Einbettung von fremden Daten und Schadcode bei Webanwendungen und Web-Services

Schlecht gesicherte Webseiten ermöglichen Angreifern, Code einzubetten, der Besucherinnen und Besucher z. B. unbemerkt auf weitere Internetseiten umleitet. Eine weitere Angriffsfläche bieten Zugriffsmöglichkeiten auf Datenbanken, die im Hintergrund der Webseite betrieben werden.
Ferner werden von Betreibenden einer Webseite häufig Tools eingesetzt, die personenbezogene Daten von Besuchern zu Werbe- oder Analysezwecken erheben. Auch diese Tools können Schwachstellen beinhalten, die Angriffsziele sein können.

6.1.4.1.1 Cross Site Scripting

Als Cross-Site-Scripting (XSS) wird eine Sicherheitslücke auf Webservern bezeichnet. Diese tritt auf, wenn eine Webanwendung nutzerseitig Daten annimmt und diese Daten dann an einen Browser weitersendet, ohne den Inhalt zu überprüfen. Damit ist es Angreifern möglich, Skripte indirekt an den Browser der Opfer zu senden und damit Schadcode auf der Seite des Clients auszuführen (s. auch „Technisches Handbuch Internet“).

Ein klassisches Beispiel für Cross-Site-Scripting ist die Übergabe von Parametern an ein serverseitiges Skript, das eine dynamische Webseite erzeugt. Dies kann etwa das Eingabeformular einer Webseite sein, wie in Webshops, Foren, Blogs und Wikis üblich. Die eingegebenen Daten werden auf der Webseite wieder als Seiteninhalt ausgegeben, wenn die Seite von Benutzern aufgerufen wird. So ist es möglich, manipulierte Daten an alle Benutzerinnen und Benutzer zu senden, sofern das Serverskript dies nicht verhindert. Diese Daten sind oft Code einer clientseitigen Skriptsprache (meist JavaScript).

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Um durch eine Webanwendung keine Basis für XSS-Angriffe zu bieten, müssen alle eingehenden Eingabewerte als unsicher betrachtet und vor der weiteren Verarbeitung auf der Serverseite geprüft werden.

6.1.4.1.2 Injection

Greift eine Anwendung auf die Daten einer SQL -Datenbank zu, so werden Befehle in Form von SQL-Anweisungen an die Datenbank übermittelt. Ist die Anwendung anfällig für SQL-Injection, können Angreifer durch Manipulation der Eingabedaten geänderte oder zusätzliche SQL-Anweisungen injizieren, die von der Anwendung an die Datenbank weitergeleitet und dort bearbeitet werden. Auf diese Weise können, wie bei einem direkten Datenbankzugriff, beliebige SQL-Anweisungen ausgeführt werden und so Sicherheitsmechanismen der Anwendung beim Datenzugriff umgangen werden.

Eine SQL-Injection kann daher z. B. die folgenden Auswirkungen haben:

- Unberechtigter Zugriff auf Daten,
- Erzeugen, Auslesen, Verändern oder Löschen von Daten,
- Ausführen von Betriebssystembefehlen,
- Kontrolle über die Datenbank

Beispiele:

1. Eine Webanwendung verwendet Eingabedaten ungefiltert zur Erzeugung von Datenbankabfragen. Dies können Angreifer ausnutzen und eine Anfrage formulieren, die neben den regulären Eingabedaten zusätzliche Befehle für die Datenbank enthält. Durch das ungefilterte Einbetten der Eingabedaten in die Datenbankabfrage werden die Befehle von der Datenbank ausgeführt. So können Angreifer direkten Zugriff auf die Datenbank erhalten.

2. Eine Webanwendung bietet eine Funktion zum Datei-Upload an und schränkt diese auf gewisse Dateitypen ein. Zur Bestimmung des Dateityps überprüft die Webanwendung ausschließlich die Dateiendung und berücksichtigt dabei nicht den Inhalt der Datei. Wird eine erlaubte Dateiendung für den Upload verwendet, können so Dateien mit beliebigem Inhalt zum Server übermittelt werden.

6.1.4.1.3 Bannerwerbung

Auf Internetseiten ist häufig Werbung zu sehen, um die Kosten für den Betrieb der Webseite zu finanzieren. Hierbei ist zwischen statischen und dynamischen Werbeeinblendungen zu unterscheiden. Statische Werbeeinblendungen bestehen aus einer Bilddatei (z. B. ein Logo) und einem damit verknüpften Link. Diese Werbung ist fest in die Webseite integriert. Dynamische Werbeeinblendungen werden von extern Anbietenden auf die Webseite geladen. Dazu lesen Anbieter mit Hilfe von Cookies das Surfverhalten - oder auch die Google-Suchanfragen - aus. Anhand der Ergebnisse sollen Nutzerinnen und Nutzern Anzeigen präsentiert werden, die auf ihre Interessen zugeschnitten sind.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Da mit der IP-Adresse ein personenbezogenes Datum ermittelt und weitergegeben wird, ist dynamische Werbung für Krankenkassen und weitere Sozialversicherungsträger nach § 67a SGB X nicht zulässig.

6.1.4.1.4 Analysesoftware (z. B. Google Analytics)

Um die Herkunft der Besucherinnen und Besucher, ihre Verweildauer auf einzelnen Seiten sowie die Nutzung von Suchmaschinen besser auswerten zu können, wird von vielen Webseitenbetreibenden ein Analysetool genutzt. Das am häufigsten verwendete Tool ist zur Zeit „google analytics“. Google kann mit diesem Analysewerkzeug ein umfassendes Benutzerprofil von Besucherinnen und Besuchern einer Webseite anlegen. Wird durch die Benutzerinnen bzw. Benutzer ein anmeldepflichtiger Google-Dienst verwendet, so kann dieses Benutzerprofil auch bestimmten Personen zugeordnet werden. Zusätzlich problematisch ist die Speicherung der Daten in den USA, welche dem Datenschutz einen geringeren Stellenwert einräumen als europäische Staaten.

Da mit der IP-Adresse mindestens ein personenbezogenes Datum ermittelt und weitergegeben wird, ist die Verwendung von „google analytics“ für Krankenkassen und weitere Sozialversicherungsträger nach § 67a SGB X nicht zulässig. Über die Datenschutzkonformität weiterer Analysetools kann hier keine Auskunft gegeben werden. Die von den Tools erhobenen Daten sowie deren weitere Verarbeitung sind der Dokumentation der jeweiligen Software zu entnehmen.

6.1.4.1.5 CMS Content Management System

Ein Content-Management-System (kurz CMS, deutsch Inhaltsverwaltungssystem) ist eine Software zur gemeinschaftlichen Erstellung, Bearbeitung und Organisation von Inhalten (Content) zumeist in Webseiten, aber auch in anderen Medienformen. Diese können aus Text- und Multimedia-Dokumenten bestehen. Personen mit Zugriffsrechten können ein solches System in den meisten Fällen mit wenig Programmier- oder HTML-Kenntnissen bedienen, da die Mehrzahl der Systeme über eine grafische Benutzeroberfläche verfügen. Besonderer Wert wird bei CMS auf eine medienneutrale Datenhaltung gelegt. So kann ein Inhalt auf Wunsch beispielsweise als PDF- oder als HTML-Dokument abrufbar sein; die Formate werden bei volldynamischen Systemen erst bei der Abfrage aus der Datenbank generiert.

6.1.4.1.6 Benutzerverwaltung

Um unberechtigte Änderungen zu verhindern und Änderungen nachvollziehen zu können, müssen sich die Benutzerinnen und Benutzer authentifizieren und bekommen anhand eines Berechtigungskonzepts Benutzerrollen zugewiesen. Hierbei wird meist hierarchisch unterschieden. So können etwa bestimmte Editoren Artikel anlegen, müssen aber von Administratoren freigeschaltet werden. Ein vertikales Rollensystem erlaubt dann bestimmten Benutzergruppen nur in bestimmten Bereichen zu arbeiten (z. B. Abteilung).

Diese Rollen- und Rechtestruktur kann einfache Freigaben nach dem Vier-Augen-Prinzip oder komplexe Workflows abbilden. An solchen Workflows können sich mehrere Personen mit verschiedenen Aufgaben beteiligen, z. B. Autoren, Editoren und Webmaster, die Inhalte erzeugen, genehmigen oder freischalten. Hier spricht man von

Redaktionssystemen. Durch Mandantenfähigkeit können mehrere unabhängige Webseiten betrieben werden.

6.1.4.1.7 Zugriffsschutz

Es wird empfohlen, die unter Ziffer 6.1.2.2 genannten Maßnahmen für die Kennwortsicherheit zu beachten.

6.1.5 Datensicherung

Neben der obligatorischen Datensicherung der technischen Infrastruktur ist bei der Datensicherung einer Internetpräsenz darauf zu achten, dass ggf. kryptologische Komponenten (z. B. zur verschlüsselten Übertragung oder zum Schutz von Benutzeranmeldungen) mitgesichert werden.

Es muss sehr genau überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen, da jede Schlüsselkopie eine potentielle Schwachstelle ist.

Hierbei ist grundsätzlich zu beachten:

- Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht unbemerkt auslesen können. Beispielsweise könnten Schlüssel in spezieller Sicherheitshardware gespeichert werden, die die Schlüssel bei Angriffen automatisch löscht. Falls sie in einer Software gespeichert werden, sollten sie auf jeden Fall überschlüsselt werden. Hierbei ist zu bedenken, dass die meisten Standard-Anwendungen, die Schlüssel oder Passwörter in der Anwendung selbst speichern, im Allgemeinen ein leichter zu brechenden Verfahren nutzen. Als weitere Variante kann auch das Vier-Augen-Prinzip bei der Schlüsselspeicherung genutzt werden, also die Speicherung eines Schlüssels in Schlüsselhälften oder Schlüsselteilen.
- Von Kommunikationsschlüsseln und anderen kurzlebigen Schlüsseln sollten keine Kopien erstellt werden. Damit eine unautorisierte Nutzung ausgeschlossen ist, sollten von privaten Signaturschlüsseln grundsätzlich keine Kopien existieren. Falls jedoch für die Schlüsselspeicherung eine reine Softwarelösung gewählt wurde, d. h. wenn keine Chipkarte oder andere Hardwarekomponenten verwendet werden, ist das Risiko des Schlüsselverlustes erhöht, z. B. durch Bitfehler oder Festplattendefekt. In diesem Fall ist es unter Umständen weniger aufwendig, eine ausreichend gesicherte Möglichkeit der Schlüsselhinterlegung zu schaffen, als bei jedem Schlüsselverlust alle Kommunikationspartner zu informieren.
- Von langlebigen Schlüsseln, die z. B. zur Archivierung von Daten oder zur Generierung von Kommunikationsschlüsseln eingesetzt werden, sollten auf jeden Fall Sicherungskopien angefertigt werden.

Besondere Sorgfalt ist bei der Datensicherung von verschlüsselten Daten bzw. beim Einsatz von Verschlüsselung während der Datenspeicherung notwendig. Treten hierbei Fehler auf, sind nicht nur einige Datensätze, sondern meist alle Daten unbrauchbar.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Die Langzeitspeicherung von verschlüsselten oder signierten Daten bringt viele zusätzliche Probleme mit sich. Es muss nicht nur sichergestellt werden, dass die Datenträger regelmäßig aufgefrischt werden, auch müssen noch die technischen Komponenten zum Verarbeiten dieser Daten zur Verfügung stehen. Ferner haben die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik zu entsprechen. Bei der langfristigen Archivierung von Daten (ohne rechtliche Relevanz, für die eine Signierung zwingend vorgeschrieben ist) kann es daher sinnvoller sein, diese unverschlüsselt zu speichern, sie aber dafür entsprechend sicher zu lagern, also z. B. in Tresoren.

Die verwendeten Kryptomodule sollten vorsichtshalber immer archiviert werden, da die Erfahrung zeigt, dass auch noch nach Jahren Daten auftauchen, die nicht im Archiv gelagert waren.

Um die kurzfristige Wiederherstellung einer Internetpräsenz sicherzustellen, ist neben der Datensicherung auch regelmäßig die Datenrekonstruktion zu proben.

6.1.6 Penetrationstest/Prüfung der Sicherheit der Webseite durch externe Tester

Angriffe auf IT-Systeme treten fast täglich auf. Um sich hiervor optimal zu schützen, ist es hilfreich, wenn man sich neben den üblichen Sicherheitsvorkehrungen zusätzlich auf die Sicht von Angreifern einlässt.

Hierfür sind Penetrationstests ein geeignetes Verfahren, um die aktuelle Sicherheit eines IT-Netzes, eines einzelnen IT-Systems oder einer (Web-)Anwendung festzustellen. Sie dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs einzuschätzen und dadurch die Wirksamkeit der vorhandenen Sicherheitsmaßnahmen zu überprüfen sowie ggf. weitere notwendige Sicherheitsmaßnahmen abzuleiten.

Durch die Prüfungen wird aufgezeigt, welche Schwachstellen zum Prüfzeitpunkt mit vertretbarem Untersuchungsaufwand und den vereinbarten Methoden gefunden werden können. Um langfristig einen guten Sicherheitseindruck über die IT-Systeme zu gewinnen, wird empfohlen, die Tests in regelmäßigen Abständen zu wiederholen.

6.2 Sichere Datenübertragung

Da im Internet die Datenpakete von einem Rechner zum nächsten weitergeleitet werden, kann jeder Rechner auf dem Weg des Datenpakets dessen Inhalt lesen und sogar verändern. Ein Rechner kann auch Datenpakete im Namen eines anderen Rechners versenden, indem er dessen Adresse als „Absender“ einträgt. Um Daten sicher von der Webseite zu deren Besucherinnen und Besuchern und zurück übertragen zu können, ist eine verschlüsselte Übertragung notwendig. Hierzu baut der Client eine Verbindung zum Server auf. Der Server authentisiert sich gegenüber dem Client mit einem

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Zertifikat. Der Client überprüft die Vertrauenswürdigkeit des Zertifikats und ob der Servername mit dem im Zertifikat hinterlegten übereinstimmt. Optional kann sich der Client mit einem eigenen Zertifikat auch gegenüber dem Server authentisieren. Dann schickt entweder der Client dem Server eine mit dem öffentlichen Schlüssel des Servers verschlüsselte geheime Zufallszahl, oder die beiden Parteien berechnen z.B. mit dem Diffie-Hellman-Schlüsselaustausch ein gemeinsames Geheimnis. Aus dem Geheimnis wird dann ein kryptographischer Schlüssel abgeleitet. Dieser Schlüssel wird in der Folge benutzt, um alle Nachrichten der Verbindung mit einem symmetrischen Verschlüsselungsverfahren zu verschlüsseln und zum Schutz von Nachrichten-Integrität und Authentizität durch einen Message Authentication Code abzusichern.

Zur Zeit der Erstellung dieses Prüfleitfadens ist das o. g. genannte Verfahren ausreichend sicher, um eine gesicherte Datenübertragung zu gewährleisten. Voraussetzung ist die ordnungsgemäße Implementierung einer Verschlüsselungssoftware auf dem Webserver. Eine Sicherheitslücke sind Konfigurationsfehler des Servers. Bei falscher Konfiguration setzt z.B. der Server die Verschlüsselung immer weiter herab, da ein Angreifer vortäuschen kann, dass der Browser des Benutzers keine Verschlüsselung beherrscht. („downgrade der Verschlüsselung auf 0 Bits“)

Zudem ist es notwendig, die Versorgung der Software mit aktuellen Updates zu beachten. Weiterhin sollte regelmäßig geprüft werden, ob die Schlüssellängen sowie die Verschlüsselungsalgorithmen dem Stand der Technik und den Sicherheitsanforderungen von Sozialdaten entsprechen.

6.2.1 Transportverschlüsselung TLS

Transport Layer Security (TLS) ist eine Weiterentwicklung von Secure Sockets Layer (SSL) und wird dazu verwendet, Informationen während der Übertragung in Netzen, in der Regel zwischen Serverdiensten und Clients oder zwischen Serverdiensten, untereinander kryptographisch abzusichern. Clients können die Verschlüsselung über SSL/TLS nur dann nutzen, wenn diese von den Serverdiensten unterstützt wird. SSL/TLS kann dazu eingesetzt werden, Informationen aus der Anwendung verschlüsselt über Netzwerkprotokolle zu übertragen. Überdies können mittels SSL/TLS auch sichere VPNs (Virtuelle Private Netze) aufgebaut werden.

Eine konzeptionelle Schwachstelle der Transportverschlüsselung ist die Verwaltung der Zertifikate und der daraus resultierenden Schlüssel. In der Vergangenheit wurden bereits mehrfach Zertifikate von einer ausstellenden Stelle gestohlen oder gefälscht. Diese ungültigen Zertifikate werden in Sperrlisten (oder teilweise als Patches der Serverhersteller) veröffentlicht, die von den Betreibenden des Webservers aktualisiert werden müssen.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

6.3 Sichere Datenannahme

6.3.1 Virenscanner

Ebenso wie Clientrechner können auch Webserver – und damit auch die bereitgestellten Inhalte - mit Schadsoftware infiziert werden. Da zwischen den Webservern und der weiteren IT-Infrastruktur noch verschiedene Sicherheitsmaßnahmen (siehe DMZ) durchgeführt werden, ist das Risiko einer Infektion des internen Netzwerkes gering. Eine Webseite die die Rechner der Besuchenden mit Viren infiziert, dürfte allerdings eine negative Berichterstattung hervorrufen, die alle Bemühungen einen erfolgreichen Internetauftritt zu erstellen, zunichtemachen.

6.3.2 Firewall/IDS (intrusion detection system)

Der Webserver muss, um seine Aufgaben erledigen zu können, direkt aus dem Internet erreichbar sein. Daher ist ein Webserver auch das erste Ziel von Angriffen aus dem Netz. Wenn die Absicherung von Webservern fester Bestandteil der IT-Sicherheitsinfrastruktur ist, wird die gesamte IT-Umgebung deutlich sicherer. Ein technisch leicht zu realisierender Angriff ist eine DOS- (denial of service) Attacke gegen den Webserver. Hierbei wird der Webserver mit so vielen Anfragen und Seitenaufrufen bombardiert, dass die Webseiten wegen Überlastung des Servers nicht mehr erreichbar sind. Eine gut konfigurierte Firewall , die z. B. massenhafte Anfragen von immer den gleichen IP-Adressen blockiert, kann in Zusammenarbeit mit dem IDS den Angriff gegen einen Webserver zumindest abschwächen und dafür sorgen, dass die Webseiten erreichbar bleiben. Empfehlenswert ist die zusätzliche Nutzung einer Web Application Firewall. Diese ist in der Lage, für jede Anwendung auf dem Webserver zulässige und nicht zulässige Anfragen zu identifizieren. Beispielsweise kann dadurch verhindert werden, dass Angreifer verschiedene mögliche Schwachstellen durch einfaches ausprobieren suchen. Die Web Application Firewall verwirft einfach alle Anfragen, die nicht in den Eingabe- und Wertefeldern der Webanwendung vorgesehen sind.

6.3.3 DMZ (Demilitarisierte Zone – „Burggraben“ zwischen Internet und eigenem Netzwerk)

Das BSI empfiehlt in seinen IT-Grundschutz-Katalogen ein zweistufiges Firewall-Konzept zum Internet. In diesem Fall trennt eine Firewall das Internet von der DMZ und eine weitere Firewall die DMZ vom internen Netz. Dadurch kompromittiert eine einzelne Schwachstelle noch nicht gleich das interne Netz. Im Idealfall sind die beiden Firewalls von verschiedenen Herstellern, da ansonsten eine bekannte Schwachstelle ausreichen würde, um beide Firewalls zu überwinden.

Die Filterfunktionen können aber durchaus von einem einzelnen Gerät übernommen werden; in diesem Fall benötigt das filternde System mindestens drei Netzanschlüsse: je

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

einen für die beiden zu verbindenden Netzsegmente (z. B. WAN und LAN) und einen dritten für die DMZ.

Auch wenn die Firewall das interne Netz vor Angriffen eines kompromittierten Servers aus der DMZ schützt, sind die anderen Server in der DMZ direkt angreifbar, solange nicht noch weitere Schutzmaßnahmen getroffen werden. Dies könnte z. B. eine Segmentierung in VLANs (Virtuellen Netzwerken) sein oder Software Firewalls auf den einzelnen Servern, die alle Pakete aus dem DMZ-Netz verwerfen.

Ein Verbindungsaufbau sollte grundsätzlich immer aus dem internen Netz in die DMZ erfolgen, niemals aus der DMZ in das interne Netz. Eine übliche Ausnahme hiervon ist der Zugriff aus der DMZ auf Datenbankserver im internen Netzwerk.

Zu dem Komplex DMZ sind keine Prüffragen genannt, da die Bewertung einer DMZ derart spezialisierte technische Kenntnisse erfordert, dass dies innerhalb der Prüfung von Internetseiten eines Sozialversicherungsträgers nicht zu leisten ist.

zur Checkliste

7 DATENSICHERHEIT (BENUTZER)

7.1 Auswertung des Benutzerverhaltens

7.1.1 Cookies

Cookies können eine Gefahr, bzw. ein Datenschutzproblem für die Benutzerinnen und Benutzer darstellen, da die Möglichkeit besteht, dass diese auch private Informationen wie Benutzernamen oder Kennwörter speichern. Durch die Webseite eines Sozialversicherungsträgers sollten Cookies nicht oder nur für die Dauer des Seitenaufrufs gesetzt werden. Ob durch einen Webseite ein Cookie gesetzt wurde, kann im Verlauf der Prüfung im Webbrowser überprüft werden. Die Anleitung hierzu kann für alle Browsertypen problemlos im Internet gefunden werden.

Cookies stellen eine Möglichkeit dar, Informationen für bestimmte Webseiten lokal in einem speziellen Dateiverzeichnis auf dem Internet-Client zu speichern. Sie dienen der zeitlich beschränkten Archivierung von Informationen. Cookies können beispielsweise von Betreibenden von Webseiten genutzt werden, um Benutzereinstellungen für personalisierte Webangebote oder "Einkaufskörbe" in Onlineshops zu realisieren oder auch um zielgruppenorientierte Werbung zu platzieren.

Teilweise sind die Informationen nicht im Cookie selbst gespeichert. Vielmehr wird im Cookie eine Art Seriennummer gespeichert, über die bei den Webseiten-Betreibenden vorliegende Informationen Benutzerinnen und Benutzern zugeordnet werden können. Ein Cookie enthält typischerweise

- Informationen über die Webseiten, an die es zurückgeschickt werden soll (beispielsweise nur an den Server, von dem es erzeugt wurde oder an alle Server in der Domain des Servers, von dem es erzeugt wurde),
- eine Gültigkeitsdauer (beispielsweise nur für die laufende Browsersitzung oder bis zu einem vorgegebenen Ablaufdatum) und
- andere, vom Betreibenden des Webservers frei bestimmbare Daten, etwa eine Benutzer-Kennung oder eine Session- ID.

7.1.2 Auswerten von Browserdaten

Die browserinternen Daten der Internetnutzer ermöglichen die Erstellung von Nutzungsprofilen. Die Auswertung beim Besuch einer Webseite verletzt das Recht der Nutzerinnen und Nutzer auf die informationelle Selbstbestimmung. Auf der Webseite eines Sozialversicherungsträgers sind derartige Auswertungen zu unterlassen. Auch externe Tools zur Analyse des Besucherverhaltens einer Webseite (z. B. Google Analytics) sind kritisch zu betrachten.

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Browser sammeln auch intern Daten über die Internet-Nutzung der verschiedenen Benutzerinnen und Benutzer, beispielsweise über History (Liste der zuletzt besuchten Internetseiten), Cache, Download-Übersichten, gespeicherte Such- und Formulardaten und Passwörter. Die Benutzerinnen und Benutzer von Browsern müssen darüber informiert sein, wo auf ihren lokalen IT -Systemen diese Daten gespeichert werden und wie sie diese löschen können. Zudem muss sichergestellt sein, dass nur Befugte darauf Zugriff haben. Bei den meisten Browsern ist es möglich, alle Daten und Dateien, die auf das persönliche Surfverhalten zurückschließen lassen, per Mausklick oder automatisch beim Beenden zu löschen.

Die Dateien auf Proxy-Servern sind besonders sensibel, da auf einem Proxy-Server alle externen Internet-Zugriffe aller Mitarbeiterinnen und Mitarbeiter protokolliert werden, inklusive der IP-Adresse des Clients, der die Anfrage gestartet hat, und der nachgefragten URL . Mit Hilfe der IP-Adresse des Clients ist es in der Regel möglich, auf konkreten Mitarbeiterinnen und Mitarbeiter zurückzuschließen. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutzverletzungen nach sich ziehen.

Von den meisten Browsern werden viele Informationen über die Benutzerinnen und Benutzer und ihr Nutzerverhalten gesammelt, von denen diese vielleicht nicht wollen, dass sie weitergegeben werden. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene Webseiten bzw. Informationen im Cache,
- History-Datenbank bzw. URL-Liste,
- Cookie-Liste,
- Informationen über Benutzerinnen und Benutzer, die im Browser gespeichert und eventuell auch weitergegeben werden.

zur Checkliste

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 0, VERTRAGLICHE VORAUSSETZUNGEN

Beantwortung durch die Revision

Prüffrage	Bemerkungen	ja	nein
Beinhaltet der Vertrag präzise Aussagen zur zu erstellenden Software, der Benutzeranleitung, zum Quellcode, zur Dokumentation und weiterer Unterlagen?			
Wurde der Vertragsgegenstand und Einsatzbereich präzise und für einen sachverständigen Dritten ausführlich und verständlich beschrieben?			
Enthält der Vertrag ein Pflichtenheft, das von beiden Vertragspartnern gemeinsam erstellt wurde?			
Enthält das Pflichtenheft alle erforderlichen Informationen über das Anwendungsgebiet, der Hard- und Softwareumgebung etc., für das die Software entwickelt werden soll?			
Wurde das Pflichtenheft von den Vertragspartnern mit Datumsangabe rechtsverbindlich unterzeichnet? (Dies gilt auch für etwaige nachfolgende Änderungen im Pflichtenheft, auf die sich die Vertragspartner unter Vereinbarung abgeänderter Vertragsbedingungen oder unter Aufrechterhaltung der bestehenden schriftlich verständigt haben.)			
Wurde im Pflichtenheft ein Qualitätsstandard definiert? (Mindeststandard sind die im Zeitpunkt der Auftragserteilung bestehenden neuesten allgemein zugänglichen Erkenntnisse der Informationstechnik.)			
Ist im Vertrag ein verbindlicher Fertigstellungstermin einschließlich Folgen bei Fristüberschreitung enthalten? (Bei erheblichen Vertragsänderungen, die der Auftraggeber nach der Erstellung des Pflichtenheftes beauftragt hat, ist die Vereinbarung hinfällig. Regelungen wären im Pflichtenheft aufzunehmen und ein neuer Termin verbindlich festzulegen.)			
Ist im Vertrag geregelt, ob die Software nur zu übermitteln ist? Anderenfalls: Wurde eine Frist vereinbart, bis zu dem die Software auf der genau zu bezeichnenden Hardware des Auftraggebers zu installieren ist und ablauffähig ist?			

Hat der Auftragnehmer dem Auftraggeber ein ausschließliches, unbefristetes, übertragbares, unwiderrufliches Nutzungsrecht an der Nutzung der Software, der Dokumentation und Benutzungsanleitung eingeräumt? (Das Nutzungsrecht gilt für alle bekannten Nutzungsarten einschließlich der Bearbeitung, Vervielfältigung und Veröffentlichung.)			
Ist geregelt, dass die Software ausschließlich für den Auftraggeber entwickelt wird und auch nicht nach Ablauf einer Frist an Dritte veräußert werden darf?			
Sind alle Vertragsänderungen nach Vertragsabschluss und die mit ihr in Zusammenhang stehenden Zusatzvereinbarungen schriftlich festgelegt worden? (Preisänderung, Liefertermin, verbindliche Unterschrift)			
Enthält der Vertrag Vereinbarungen über die Einweisung/ Benutzung des Softwareprogramms? (Dauer/Ort/Preis)			
Ist die Abnahme der Software verbindlich geregelt? (Die Abnahme ist nach Übergabe der zur Software gehörenden Unterlagen (Quellcode/Dokumentation) zu erklären und in einem von den Vertragspartnern zu unterzeichnenden Abnahmeprotokoll festzuhalten. Ggf. ist eine Testphase zu vereinbaren.)			
Enthält der Vertrag Regelungen zum Schadensersatz bzw. Fristverlängerung, wenn die Abnahme nicht erfolgen kann?			
Ist verbindlich geregelt, welchen Zugriff / bzw. Eigentumsrechte der Auftraggeber auf den Quellcode hat und wie der Auftragnehmer den Quellcode verwaltet?			
Ist die Aufbewahrungsfrist für Quellcodes etc. im Vertrag geregelt, sofern diese beim Auftragnehmer verbleiben?			
Ist (gemäß EVB-IT) verbindlich geregelt, dass beschaffte Hard-und Software keine Funktionen • zum unerwünschten Absetzen/Ausleiten von Daten enthält? • zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik enthält? • zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen enthält?			

Zum Text

ANLAGE 1, GESTALTUNG DER INTERNETSEITE

Beantwortung durch die Revision

Prüffrage	Bemerkungen	ja	nein
Ist die Internetseite im Browserfenster komplett sichtbar, so dass horizontales scrollen nicht erforderlich ist?			
Ist der Seitenaufruf ohne Zusatzsoftware möglich?(erkennbar an einer Installationsaufforderung)			
Ist der Seiteninhalt mit einem Standardbrowser sichtbar?			
Sind filmähnliche Vor- und Abspanne abschalt- bzw. überspringbar?			
Ist die Navigation und Struktur der Website einfach und logisch?			
Können sich die Benutzerinnen und Benutzer überall auf der Website leicht und schnell orientieren? (keine umfangreichen Verzweigungen in Unterseiten)			
Beeinträchtigt die Farbgestaltung des Hintergrundes die Lesbarkeit von Texten und die Nutzbarkeit von Bildinformationen nicht?			
Sind alle Links sind deutlich erkennbar?			
Ist ein Link zur Startseite auf jeder Seite vorhanden?			
Funktionieren die geprüften Links?			
Ist die Startseite so gestaltet, dass die Besucher die Inhalte des Onlineangebotes auf einen Blick erkennen können?			
Sind die Texte prägnant, einfach verständlich und für das Internet optimiert (nicht zu lang)?			
Werden Schriftarten und -größen durchgängig einheitlich genutzt?			
Werden für angebotene Downloads Dateigrößen bzw. Ladezeiten angegeben?			
Sind die stichprobenartig geprüften Webinhalte rechtlich korrekt?			
Ist die nach § 5 TMG vorgeschriebene Anbieterkennzeichnung vorhanden (Impressum)?			
Ist der Text der Webseite gendergerecht verfasst?			
Werden die obigen Anforderungen auch in der mobilen Darstellung erfüllt?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 2, BARIEREFREIHEIT

Beantwortung durch die Revision

Prüffrage	Bemerkungen	ja	nein
Welche Normen oder Standards wurden bei der Sicherstellung der Barrierefreiheit beachtet?			
Werden zur reinen Texteinrückung keine Listen und Listenelemente verwendet?			
Wird eine dem Inhalt angemessene, einfache und klare Sprache benutzt?			
Sind Abkürzungen / Akronyme beim ersten Auftreten ausgeschrieben?			
Sind die Schriftgrößen variabel?			
Werden Unterstreichungen nur für Links verwendet?			
Heben Hintergrund und Schrift sich kontrastreich voneinander ab?			
Wird auf animierte Grafiken verzichtet?			
Sind Grafiken mit aussagekräftigen Alternativtexten beschrieben? **Ausnahme:** Grafiken ohne informative Funktionen, z. B. Farbflächen, dekorative Farbübergänge und Schmuckgrafiken			
Sind mit Farbe dargestellte Informationen auch ohne Farbe nutzbar bzw. stützen sich nicht ausschließlich auf Farbangaben?			
Werden problematische Farbkombinationen vermieden(rot/grün, kontrastarme Farben)?			
Sind grafische Bedienelemente (Pfeile u.ä) mit aussagekräftigen Alternativtexten versehen, die auch das Ziel des Links bezeichnen?			
Ist eine Inhaltsübersicht (z.B. Sitemap) oder eine ähnliche Orientierungshilfe vorhanden?			
Ist das Ziel von Hyperlinks eindeutig identifizierbar (keine Formulierungen wie „Klicken Sie hier“, sondern nur Links mit beschreibendem Text)?			
Ist das Datenformat der verlinkten Datei bei Links auf nicht-HTML-Seiten beschrieben (z. B. PDF, Word, usw.)?			
Werden Linkziele durch informative „title“-Attribute klargestellt (z. B. Link öffnet PDF-Datei in neuem Fenster)?			
Ist das Angebot auch ohne Maus, also nur mit der Tastatur bedienbar?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Wird auf automatische Popup-Fenster verzichtet und erfolgt das Öffnen neuer Fenster mit Ankündigung?			
Sind lange Texte durch Zwischenüberschriften gegliedert? Wurde die Überschriften-Hierarchie eingehalten? (erst Überschrift 1, dann Überschrift 2, …)			
Wird auf flackernde, blinkende oder sich bewegende Elemente (z. B. Laufschriften) verzichtet?			
Sind bei Datentabellen Zeilen- und Spaltenüberschriften gekennzeichnet? (zur Kennzeichnung werden <td> für Datenzellen und <th> für Überschriften verwendet)			
Sind Formularfelder durch das Element <fieldset> gruppiert und damit in logische Blöcke eingeteilt?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 3, RECHTLICHE VORAUSSETZUNGEN BEIM BETRIEB EINER WEBSEITE

Beantwortung durch die Revision

Prüffrage	Bemerkungen	ja	nein
Ist die Verwendung der Inhalte der Webseite Urheberrechtlich unbedenklich bzw. vertraglich geregelt? (s. Antworten der Webseitenbetreiber)			
Werden die nach § 5 Telemediengesetz notwendigen Inhalte des Impressum auf der Webseite wiedergegeben? • Name • Anschrift • Rechtsform • Vertretungsberechtigte Person • Kontaktadresse postalisch • Kontaktadresse elektronisch • Angaben zur zust. Aufsichtsbehörde • In Fällen, in denen eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung vorliegt, die Angabe dieser Nummer			
Ist das Impressum auf der Webseite leicht erkennbar / leicht aufzufinden?			
Sind die Verlinkungen aus wettbewerbsrechtlicher Betrachtungsweise in Ordnung? (keine kommerzielle Werbung)			
Ist bei journalistisch-redaktionell gestalteten Angeboten (Mitgliederzeitschrift) eine verantwortliche Person benannt? • Name • Anschrift			
Bei mehreren Verantwortlichen: • Sind alle Verantwortlichen aufgeführt? • Ist erkennbar, für welchen Teil des Angebotes die jeweils benannte Person verantwortlich ist?			
Sind die Vorgaben gem. § 55 RStV (Rundfunkstaatsvertrag) eingehalten?			
Werden verlinkte Inhalte Dritter regelmäßig auf ihre Unbedenklichkeit geprüft? (s. Antwort der Webseitenbetreiber)			
Ist das Impressum aktuell?			
Ist eine Datenschutzerklärung vorhanden? • Sind alle vorgeschriebenen Inhalte			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

enthalten? • Sind ggf. Änderungen durch das Inkrafttreten der DSGVO berücksichtigt?			
Ist der Auftraggeber der Internetseite auch Eigentümer der Domain? (Abfrage bei www.denic.de)			

Zum Text

RECHTLICHE VORAUSSETZUNGEN BEIM BETRIEB EINER WEBSEITE

Beantwortung durch Webseitenbetreiber

Prüffrage	Bemerkungen	ja	nein
Wurde vor der Einrichtung der Domain geprüft, ob der Domainname möglicherweise die Rechte Dritter verletzt?			
Liegen ggf. Verträge für die Nutzungsrechte von Bildern vor?			
Liegen ggf. Verträge für die Nutzungsrechte von Fotos vor?			
Liegen ggf. Verträge für die Nutzungsrechte von Kartenmaterial vor?			
Liegen ggf. Verträge für die Nutzungsrechte von Videos vor?			
Liegen ggf. Verträge für die Nutzungsrechte von Texten (Zitaten) vor?			
Liegt bei Fotos von Personen eine Einverständniserklärung zur Veröffentlichung vor?			
Sind die verwendeten Schriftarten frei verfügbar? Falls nicht, liegt ein Vertrag für die Nutzung vor?			
Bei Gestaltung einer Webseite durch Dienstleister: ist die Beachtung von Urheberrechten Vertragsgegenstand?			
Wurde überprüft, ob die Dienstleister selbst über die notwendigen Rechte der auf der Webseite verwendeten Inhalte verfügen?			
Verweisen Links zu weiteren Webseiten auf rechtlich bzw. urheberrechtlich unbedenkliche Inhalte?			
Werden verlinkte Inhalte Dritter regelmäßig auf Unbedenklichkeit geprüft?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 4, DATENSCHUTZERKLÄRUNG

Beantwortung durch die Revision / den Datenschutzbeauftragten

Prüffrage	Bemerkungen	ja	nein
Existiert auf der Webseite eine Datenschutzerklärung?			
Ist diese leicht auffindbar / von jeder Seite aus zu erreichen?			
Enthält die Datenschutzerklärung die Art der gespeicherten Daten gemäß DSGVO? (Auswahl häufig erhobener Daten:) • Name der abgerufenen Datei • Datum und Uhrzeit des Abrufs • übertragene Datenmenge • Meldung, ob der Abruf erfolgreich war • IP-Adresse			
Wird der Grund der Datenspeicherung genannt?			
Werden Empfängerinnen und Empfänger der gespeicherten Daten benannt?			
Wird die Weitergabe der Mailadressen ausgeschlossen?			
Wird eine Aufbewahrungsfrist für die gespeicherten Daten genannt?			
Werden Nutzungsdaten nach Inanspruchnahme der Leistung – hier nach Besuch einer Internetseite – gelöscht?			
Bei Inanspruchnahme eines Dienstleisters für den Betrieb des Webservers: • Ist die Einhaltung der Datenschutzerklärung vertraglich geregelt? • Wird die Einhaltung der Datenschutzerklärung geprüft?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Datenschutzerklärung

Beantwortung durch Webseitenbetreiber / die verantwortliche Stelle

Prüffrage	Bemerkungen	ja	nein
Wer sind die Empfängerinnen und Empfänger der gespeicherten Daten? • **Bitte Angeben**			
Werden beim Besuch der Seite Cookies gesetzt? • Werden diese nach dem Besuch der Seite gelöscht? • Ist sichergestellt, dass aus den Cookies keine Rückschlüsse auf das Nutzerverhalten gezogen werden? • Wird der Besucher auf evtl. gesetzte Cookies hingewiesen?			
Wird die IP-Adresse der Besucherinnen und Besucher nach Verlassen der Seite gelöscht?			
Bei Mailkontakt: Werden die Mailadressen ausschließlich für die Korrespondenz genutzt?			
Ist die Weitergabe der Mailadressen sowie die Verwendung für Werbezwecke ausgeschlossen? • Wie wird dies sichergestellt?			
Bei Inanspruchnahme eines Dienstleisters: • Ist die Einhaltung der Datenschutzerklärung vertraglich geregelt? (bitte Unterlagen / Auszug aus Vertrag beifügen) • Wird die Einhaltung der Datenschutzerklärung geprüft? (Bitte die Belege / Dokumentation der letzten 2 Prüfungen beifügen)			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 5, DATENSCHUTZGRUNDVERORDNUNG DSGVO

Prüffrage	Bemerkungen	ja	nein
Allgemein			
Sind relevante Unterlagen, Dienstanweisungen u.a. rechtzeitig von in Kraft treten der DSGVO angepasst worden? Z.B. - Dienstanweisung Datenschutz - Datenschutzverpflichtung - Einwilligungserklärungen - Technische und Organisatorische Maßnahmen - Verarbeitungsverzeichnisse			
Einwilligung			
Wird der Nutzer **vor** Besuch der Internetseite aufgefordert, aktiv seine Einwilligung zur Speicherung personenbezogener Daten zu erklären?			
Ist diese Aufforderung zur Einwilligung verständlich und erklärt?			
Geht aus der Aufforderung zur Einwilligung verständlich und vollständig hervor, welche Daten verarbeitet, gespeichert und ggf. weitergeleitet werden?			
Ist erkennbar, welche Dienste auf diese Daten Zugriff haben?			
Gibt es die Möglichkeit, diese Einwilligung zu widerrufen?			
Ist dieser Widerruf ebenso klar und eindeutig wie die Einwilligung gestaltet?			
Ist die Möglichkeit zum Widerruf auf der Internetseite leicht auffindbar?			
Technische und Organisatorische Maßnahmen (TOM)			
Ist im Bezug auf die Internetseite eine Risikobewertung durchgeführt worden?			
Sind die einzelnen technischen und organisatorischen Maßnahmen an die Ergebnisse der Risikobewertung angepasst worden?			
Zugangskontrolle: Sind Kennwortrichtlinien, Benutzerverwaltung und entspr. Dienstanweisungen aktuell gehalten?			
Datenträgerkontrolle: Ist durch TOM sichergestellt, dass alle Datenträger, auf denen sich personenbezogene Daten befinden (auch in Webservern, Kopiergeräten, Mobile Geräte), vor unbefugtem Zugriff geschützt sind?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

(Dienstanweisungen, Verträge, Kontrollen)			
Speicherkontrolle: Ist verhindert, dass personenbezogene Daten unbefugt geändert oder eingesehen werden? (automatische Sperrung von DV-Geräten, Monitoring von Webseiten und IT-Systemen, Sicherungssysteme für Internetanwendungen….)			
Benutzerkontrolle: Existieren nachvollziehbare und aufgabenbezogene Berechtigungskonzepte für die Administration bzw. Aktualisierung von Internetseiten			
Zugriffskontrolle: Ist beim Aufbau einer Internetseite (z.B. durch Penetrationstests) sichergestellt worden, dass Benutzer ausschließlich auf Daten zugreifen können, die Ihrer Berechtigung unterliegen und nicht aus dem Berechtigungssystem ausbrechen können?			
Übertragungskontrolle: Kann überprüft und festgestellt werden, welche auf der Internetseite eingegebenen Daten anderen übermittelt oder zur Verfügung gestellt werden? Sind Daten durch gesicherte Übertragung vor unbefugtem Zugriff geschützt?			
Eingabekontrolle: Wird durch Protokollierung festgehalten, welche Daten durch welche Nutzer eingegeben oder verändert worden sind? Ist sichergestellt, dass auch die Speicherung der Protokolldateien die Anforderungen an den Datenschutz erfüllt?			
Transportkontrolle: Sind personenbezogene Daten beim Transport von Datenträgern, aber auch von Akten und über Datenleitungen vor unbefugten Zugriff geschützt? (verschlossene Behältnisse, Transportverschlüsselungen, aber auch Vertragsgestaltungen mit externen Anbietern)			
Wiederherstellbarkeit: Ist geplant, wie im Störungsfall die IT-Systeme geregelt abgeschaltet und funktionsfähig wieder hochgefahren werden können? Sind diese Planungen den Verantwortlichen bekannt gemacht worden?			
Zuverlässigkeit: Werden Systemzustände über Monitoring überwacht? Werden die entstehenden Protokolldaten regelmäßig ausgewertet und entsprechende			

Maßnahmen eingeleitet? Werden die Systemparameter wie Betriebszustand, Systemalter, Ausfallhäufigkeit usw. überwacht und Neuanschaffungen entsprechend geplant?			
Datenintegrität: Sind Vorkehrungen getroffen, um die Manipulation von Daten durch Fehlfunktionen oder Benutzereingriffe zu verhindern? Werden regelmäßige Sicherungen des Systems durchgeführt? Werden die Systemsicherungen regelmäßig auf ihre Funktionsfähigkeit überprüft?			
Auftragskontrolle: Sind Kontrollrechte über die Verarbeitung personenbezogener Daten vertraglich mit den Auftragnehmern vereinbart? Wird die auftragsgemäße Datenverarbeitung vom Auftraggeber regelmäßig überprüft?			
Verfügbarkeitskontrolle: Liegen Planungen und Maßnahmen zur Verhinderung von Notfällen vor? Schutz vor - Feuer - Wasser - Diebstahl - Schadsoftware - Angriffe von Innen und Außen - usw.			
Trennbarkeit: Ist sichergestellt, dass der Verarbeitungszweck bei der Datenhaltung berücksichtigt wird? Wird die Verarbeitung von Daten belegbar nur mit dem dafür vorgesehenen Datenbestand durchgeführt? Sind Maßnahmen getroffen, um die Verknüpfung von Daten mit unterschiedlichen Erhebungs- und Verarbeitungszwecken zu unterbinden?			
Speicherung von IP-Adressen: Werden die Nutzer einer Internetseite über die Speicherung von IP-Adressen informiert? Erfolgt die Information vor der Speicherung? Wir auch über die eventuelle Weitergabe der Daten informiert und die Zustimmung eingefordert?? Ist eine aktive Einwilligung erforderlich? Haben die Nutzer die Möglichkeit eines Widerrufes der Einwilligung zur Speicherung? Werden die Nutzer nach Widerruf der Einwilligung über eine Löschung der Daten informiert?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheits- und Sozialdaten) Wurde für jedes Verfahren, welches besondere Kategorien personenbezogener Daten verarbeitet, eine Risikoanalyse durchgeführt? Wurden von diesen Risikoanalysen Maßnahmen zum Schutz der Daten abgeleitet? Werden diese Maßnahmen bei Änderungen des Datenbestandes oder anderer Risikoparameter aktualisiert?			
Informationsrecht Werden betroffene Personen präzise und leicht verständlich über die Verarbeitung personenbezogener Daten informiert? Wird auf den Zweck der Verarbeitung hingewiesen? Wird ggf. auf ein Profiling aus den erhobenen Daten hingewiesen? Wird ggf. über die Weiterleitung von Daten informiert (Soz. Medien, Werbung, Statistiken)? Sind Informationen, die sich an Kinder richten, so formuliert, dass sie von diesen verstanden werden können?			
Transparenz Wird den Nutzern einer Internetseite klar und verständlich angezeigt, welche Rechte sie in Bezug auf die Speicherung personenbezogener Daten haben? Sind diese Informationen leicht auffindbar (und auch leicht verständlich, lesbar, usw.)			
Auskunft Ist der Betreiber einer Internetseite in der Lage, auf Verlangen einer betroffenen Person Auskunft über die bereits erhobenen Daten zu geben? Sind Prozesse etabliert, die es ermöglichen, diese Auskunft in vertretbarer Zeit und vertretbarem Aufwand zu erteilen?			
Berichtigung Werden die Nutzer der Internetseite darauf hingewiesen, dass sie das Recht haben, Daten ggf. berichtigen zu lassen? Kann der Webseitenbetreiber auf Verlangen einer betroffenen Person in vertretbarer Zeit / mit vertretbarem Aufwand unvollständige oder falsche Daten berichtigen bzw. ergänzen? Ist ein Prozess eingerichtet, mit dem die berichtigten Daten ggf. auch an weitere			

Verantwortliche weitergegeben werden können?			
Datenlöschung Ist der Betreiber einer Internetseite in der Lage, Daten einer betroffenen Person auf deren Verlagen zu löschen? Werden bei der Datenlöschung auch Sicherungskopien, Replikationen usw. erfasst? Wird die Person von der erfolgten Löschung unterrichtet? Existiert ein Prozess, in dem ggf. auch die weiteren Verantwortlichen von dem Verlangen nach Löschung der Daten unterrichtet werden?			
Einschränkung der Verarbeitung Ist der Betreiber der Internetseite in der Lage, die Verarbeitung von Daten in Streitfällen nach Art. 18 einzuschränken? Gibt es Regelungen, wie in diesem Fall mit den entsprechenden Daten zu Verfahren ist?			
Mitteilung über Berichtigung und Löschung Sind Verfahren eingerichtet und bekannt gegeben, wie auf Ersuchen um Berichtigung und Löschung von Daten reagiert wird? Können alle weiteren verarbeitenden Stellen von diesen Ersuchen informiert werden? Sind Datenarten gekennzeichnet, die nicht berichtigt oder gelöscht werden können, da dies unmöglich oder mit unverhältnismäßigem Aufwand verbunden ist?			
Automatisierte Entscheidungen (Dunkelverarbeitung) und Profiling Wird die betroffene Person darüber informiert, dass ihre Daten automatisiert verarbeitet werden? Wird durch eine automatisierte Verarbeitung eine für die betroffene Person negative Entscheidung getroffen – werden die in § 37 (1) BDSG (neu) genannten Voraussetzungen erfüllt? Ist vor der Einführung der automatisierten Verarbeitung besonderer Kategorien personenbezogener Daten eine Datenschutz-Folgeabschätzung vorgenommen worden? Wurden nach Durchführung der Datenschutz-Folgeabschätzung technische und organisatorische Maßnahmen eingeleitet, um ggf. festgestellt Risiken zu minimieren?			
Datenschutzfreundliche Voreinstellungen Wurde bei der Gestaltung der Internetseite			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

berücksichtigt, dass nur die Daten erfasst und verarbeitet werden, die zwingend erforderlich sind? Gewähren die Voreinstellungen von Auswahlfeldern, opt-in-Feldern („Häkchen“), Checkboxen usw. den Nutzern den größtmöglichen Datenschutz? Sind Funktionen, wie z.B. die Anmeldung für einen Newsletter so voreingestellt, dass die Wahlfreiheit der Nutzer nicht eingeschränkt ist (z.B. keine Vorauswahl in den Feldern für die Einwilligung getroffen, Standortdaten werden erst nach Einwilligung genutzt)? Wird von dem Speichern von Cookies die Einwilligung der Nutzer eingeholt?			
Verantwortlichkeiten Ist der Verantwortliche einer Internetseite in der Lage, einen Nachweis für die Einhaltung der Grundsätze nach Art 5 (1) DSGVO zu erbringen? - Rechtmäßigkeit - Treu und Glauben (Daten werden nach Art und Umfang nur so verarbeitet, wie angegeben) - Transparenz - Zweckbindung - Datenminimierung - Richtigkeit - Speicherbegrenzung - Integrität - Vertraulichkeit - Einhaltung der technischen und organisatorischen Maßnahmen			
Stand der Technik Werden in regelmäßigen Abständen Risikobewertungen bzw. Datenschutz-Folgeabschätzungen vorgenommen und Maßnahmen ergriffen, um die entdeckten Risiken zu minimieren? Entsprechen die ergriffenen Schutzmaßnahmen denen vergleichbarer Institutionen? Sind die Verantwortlichen zeitlich und von ihrer Befähigung in der Lage, die Anforderungen des Datenschutzes an z.B. einen Internetauftritt zu erfüllen? Werden die technischen Anlagen sowie die eingesetzte Software regelmäßig geprüft, ob sie den aktuellen Anforderungen an Sicherheit und Datenschutz noch entsprechen?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Auftragsverarbeitung Sind Verträge mit Auftragnehmern an die DSGVO angepasst bzw. aktualisiert worden? Ist sichergestellt, dass Auftragnehmer die Vorgaben der DSGVO beachten? Hat der Auftraggeber vertraglich ein Prüfrecht mit dem Auftragnehmer vereinbart?			
Backup- und Cloudlösungen Sind für Anbieter von Backup- und Cloudlösungen die Regelungen und vertraglichen Vereinbarungen der DSGVO für Auftragsdatenverarbeitung beachtet? Befinden sich die Standorte der Cloud-Anbieter innerhalb der EU oder in einem Drittland, welchen ein Schutzniveau garantiert, das dem der DSGVO gleichwertig ist? Liegt für den Anbieter einer Backup- oder Cloudlösung eine Zertifizierung gem. der Artikel 42, 43 DSGVO vor?			
Löschstrategien Ist ein Prozess etabliert, durch den sich das Ersuchen einer betroffenen Person auf Löschung der sie betreffenden Daten umsetzen lässt? Sind diese Daten mit vertretbarem Aufwand auffindbar? Ist die Löschung von Daten mit der verwendeten Datenstruktur vereinbar? Ist sichergestellt, dass die Daten vollständig gelöscht sind? Ist es auch bei getrennter Datenhaltung (wegen unterschiedlicher Erhebungs- und Verwendungszwecke) möglich, alle Daten aufzufinden und zu löschen? Ist sichergestellt, dass die betroffene Person von der Löschung ihrer Daten informiert wird?			
Meldung und Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten Sind im Verarbeitungsprozess Mechanismen installiert, mit denen sich eine Verletzung des Schutzes personenbezogener Daten feststellen lässt (Protokollierungen, Warnmeldungen)? Werden diese Mechanismen regelmäßig ausgewertet? Ist ein Prozess eingerichtet, mit dem ggf. die Aufsichtsbehörde innerhalb von 72 Stunden oder die betroffene Person unverzüglich informiert werden kann? Ist sichergestellt, dass die Meldepflichten auch im Rahmen der Auftragsdatenverarbeitung beachtet werden?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Datenschutz- Folgeabschätzung Wird vor der Inbetriebnahme von Verfahren, die besondere personenbezogene Daten verarbeiten, (Sozial-; Gesundheitsdaten) eine Datenschutz- Folgeabschätzung vorgenommen? Sind diese auch für bereits bestehende Verfahren nachträglich durchgeführt worden? Werden die Erkenntnisse hieraus für die Verbesserung und Absicherung der Verfahren genutzt? Werden Datenschutz- Folgeabschätzungen regelmäßig wiederholt - Nach Ablauf von 3 Jahren - Bei Änderung der Art der erhobenen Daten - Bei Änderungen der Art der Verarbeitung - Bei Veränderungen der technischen und organisatorischen Maßnahmen (wodurch sich evtl. ein Risiko mindern kann)?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 6, ABSICHERUNG DER WEBSEITEN

Beantwortung durch Webseitenbetreiber / die verantwortliche Stelle

Prüffrage	**Bemerkungen**	**ja**	**nein**
Kann ein Nachweis für einen durchgeführten Penetrationstest vorgelegt werden? • Ist dokumentiert dass eventuelle - im Penetrationstest festgestellte - Sicherheitslücken behoben wurden?			
Softwareentwickung			
Wurden die Anforderungen vor Entwicklung der Internetseiten formuliert und dokumentiert? • Lastenheft • Pflichtenheft • Leistungsbeschreibung			
Wurden bei der Formulierung der Anforderungen einzuhaltende Standards festgelegt? • Barrierefreiheit • W3C – Konformität • Sicherheit nach BSI-Gundschutz • …			
Wurde die Entwicklung abgenommen und freigegeben?			
Wurde das absolvieren der verschiedenen Teststufen dokumentiert?			
Ist mit dem Entwickler ein festgeschriebenes • Update- • Change- • Patchmanagement vereinbart?			
Allgemeine/organisatorische Maßnahmen:			
Ist die Netzwerkarchitektur der für diese Prüfung relevanten Bereiche beschrieben? • Durch welchen Betreiber wird die Infrastruktur betrieben? • Ist der Aufbau der einzelnen Systeme dokumentiert? • Ist dokumentiert, welche Verfahren auf jedem Server / jeder VM installiert sind? • Sind die Abhängigkeiten zu Vor- und Nachgelagerten Systemen dokumentiert?			
Werden neue Software bzw. neue Versionen des Internetauftritts vor Inbetriebnahme getestet? • Wie wird getestet? • Was wird getestet? • Durch wen wird getestet?			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

• Wird dies dokumentiert?			
Ist sichergestellt, dass Updates für alle relevanten Systeme (CMS, Virenscanner, Firewall, Kryptographie usw.) zeitnah installiert werden?			
Werden für die o.a. Systeme regelmäßige Informationen bezogen, um Informationen über Updates und Sicherheitslücken zu erhalten?			
Werden die Webseiten regelmäßig Server- und Clientseitig auf Auffälligkeiten geprüft?			
Wird eine Protokollierung auf den Webservern datenschutzgerecht vorgenommen? (Anonymisierung der IP.Adresse z.B. 123.123.123.xxx)			
Wird der Internetauftritt regelmäßig historisiert?			
Wurde der HTML-Code auf HTML-konforme Codierung geprüft? (W3C-Standard)			
Sind die Sicherheitsfeatures des CMS aktiviert? • Falls nein: werden Ersatzprodukte genutzt?			
Werden Logfiles regelmäßig auf Auffälligkeiten überprüft?			
Werden die Logfiles auf Logins auf der Administrationskonsole des CMS geprüft?			
Sind die Standardkennwörter und Standardnutzer der genutzten Systeme geändert worden?			
Wird durch eine Zugangssteuerung gewährleistet, dass Administrationszugänge nur aus dem eigenen Netz möglich sind?			
Wird die Webseite mit einem Integritätsscanner geprüft, um festzustellen, ob unautorisierter Code vorhanden ist?			
Wird ein Intrusion Detection/Intrusion Prevention System (IDS/IPS) genutzt um festzustellen, ob Angriffe auf die Webseite stattfinden/stattgefunden haben?			
Wird regelmäßig geprüft, ob außergewöhnlich starker Traffic auf der Webseite stattfindet?			
Sind alle Authentifizierungsdaten durch eine Verschlüsselung geschützt? • Auf dem Anmeldeserver? • Bei der Übertragung?			
Wurde vor der Einrichtung der kennwortgeschützten Bereiche der Schutzbedarf der enthaltenen Daten klassifiziert?			
Ist sichergestellt, dass Benutzernamen nicht doppelt vergeben werden?			
Werden die Anmeldedaten (Benutzername und			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Kennwort) auf dem Anmeldeserver in gesicherten Bereichen abgelegt?			
Werden die Anmeldedaten zusätzlich verschlüsselt/gehasht?			
Ist sichergestellt, dass die Anmeldedaten nicht ohne Wissen der Nutzerinnen und Nutzer als Cookie lokal auf dem Rechner gespeichert werden? • Ist die Gültigkeit evtl. gesetzter Cookies auf die Dauer der Browsersitzung begrenzt?			
Werden die aktuellen Empfehlungen des BSI für Kennwort – und Komplexitätsrichtlinien eingehalten? (Bitte die Kennwortrichtlinien beifügen.)			
Gibt es ein Konzept zur Notfallvorsorge, das die Folgen eines Ausfalls minimiert und die Handlungen im Falle eines Ausfalls vorgibt?			
Sind wichtige Aufgaben so beschrieben, dass das Gesamtsystem im Notfall, ohne vorherige Kenntnis der Systemkonfiguration, wiederhergestellt werden kann?			
Gibt es einen Wiederanlaufplan, der das geregelte Hochfahren des Systems gewährleistet?			
Ist die Notfallplanung für den Webserver in den existierenden Notfallplan integriert?			
Bei hohen Anforderungen an die vertraglich zugesicherte Verfügbarkeit: Werden Komponenten des Webservers redundant angelegt?			
Wird der Ausfall der Internet-Anbindung eingeplant?			
Bei SSL/TLS -Nutzung: Kann auf den privaten Schlüssel des SSL -Zertifikats bei einem Wiederanlauf des Systems zugegriffen werden?			
Bei SSL/TLS -Nutzung: Ist der private Schlüssel des SSL -Zertifikats durch ein Passwort geschützt und dieses Passwort sicher hinterlegt?			
Ist sichergestellt, dass eine Verschlüsselung auf einem festgelegten Level (z.B. 256 BIT) erfolgt und ein potenzieller Angreifer kein downgrade der Verschlüsselung auf 0 BIT erzwingen kann?			
SQL injection			
Werden Eingaben und Parameter vor Weiterleitung an das Datenbanksystem überprüft und gefiltert?			
Ist gewährleistet, dass keine Fehlermeldungen nach außen ausgeben werden, welche Rückschlüsse auf das verwendete System oder			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

auf die Struktur der dahinterliegenden Datenbank zulassen?			
cross site scripting			
Wird neben der SessionID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funktionen der Webanwendung benötigt?			
Werden bei Webanwendungen kritische Aktionen nur nach einer erneuten Authentisierung oder einer manuellen Interaktion ausgeführt?			
Bannerwerbung			
Werden ggf. vorhandene Anzeigen und Werbung ausschließlich durch die Verwendung von statischen Links realisiert?			
Ist sichergestellt, dass dabei keine personenbezogenen Daten erhoben werden? (IP-Adresse)			
Analyse der Besuche der Webseite			
Ist sichergestellt, dass bei der Analyse der Besucherbewegungen zur und auf der Webseite keine personenbezogenen Daten erhoben werden? (IP-Adresse anonymisiert?)			
Content Management System			
Wird das CMS mit einer nachvollziehbaren und dokumentierten Rechteverwaltung genutzt?			
Werden bei Bearbeitung unterschiedlicher Inhaltsbereiche die Berechtigungen über ein Rollensystem realisiert?			
Sind im CMS die aktuellen Kennwortempfehlungen des BSI berücksichtigt?			
Datensicherung			
Sind kryptographische Schlüssel (Zertifikate) auch bei Datensicherungen vor unbefugtem Auslesen geschützt?			
Wird bei Langzeitspeicherung verschlüsselter Daten regelmäßig geprüft, ob die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen?			
Ist sichergestellt, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann?			
Werden verwendete Kryptoprodukte archiviert?			
Werden die Konfigurationsdaten von Kryptoprodukten gesichert?			
Ist festgelegt, wie die Datensicherungen organisatorisch und technisch ablaufen?			
Entspricht das festgelegte Verfahren für die Datensicherungen den Verfügbarkeitsanforderungen?			
Wird regelmäßig getestet, ob die gesicherten			

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

Daten problemlos zurückgespielt werden können?			
Transportverschlüsselung			
Bieten alle Serverdienste, bei denen es sinnvoll und möglich ist, die Informationen verschlüsselt über SSL/TLS an?			
Ist sichergestellt, dass die eingesetzten Server kryptographische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen?			
Unterstützen die eingesetzten Server-Produkte eine sichere Version von SSL/TLS?			
Wird der private Serverschlüssel besonders geschützt?			
Virenscanner			
Ist sichergestellt, dass der Webserver sowie die bereitgestellten Inhalte regelmäßig auf Schadsoftware geprüft werden?			
Wird mindestens einmal pro Tag geprüft, ob Updates für die Schadprogramm-Signaturen verfügbar sind und werden diese Updates unverzüglich eingespielt?			
Ist sichergestellt, dass die Updates für Viren-Schutzprogramme und für Schadprogramm-Signaturen auf allen IT -Systemen eingespielt werden, auf denen das entsprechende Viren-Schutzprogramm installiert ist?			
Wird die Konfiguration des Viren-Schutzprogramms nach dem Einspielen von Engine-Updates auf Veränderungen überprüft?			
Ist die Aktualisierung der Viren-Schutzprogramme und der Schadprogramm-Signaturen in das bestehende Patch- und Änderungsmanagement integriert?			
Sind die Paketfilter-Funktionen auf allen gefährdeten IT - Systemen aktiviert?			
Firewall			
Ist der Webserver durch eine Firewall geschützt? • Wird diese durch ein Intrusion Detection System (IDS) ergänzt?			
Ist zusätzlich eine Web Application Firewall zum Schutz des Webservers eingesetzt?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ANLAGE 7, SCHUTZ DER WEBSEITENBESUCHER

Beantwortung durch Webseitenbetreiber / die verantwortliche Stelle

Prüffrage	Bemerkungen	ja	nein
Cookies			
Wird auf das Setzen von Cookies auf dem Rechner der Benutzerinnen und Benutzer verzichtet? • Falls Cookies gesetzt werden – ist die Haltbarkeit auf die Dauer der Browsersitzung begrenzt?			
Ist sichergestellt, dass die Cookies keine personenbezogenen oder Sozialdaten auf dem Rechner der Webseitenbesucher speichern?			
Ist sichergestellt, dass Cookies fremder Server nicht ausgewertet werden? (Falls google analytics oder social Media cookies „Facebook-Button“ genutzt werden – wie wird obige Anforderung sichergestellt?)			
Ist sichergestellt, dass die Browser-Session-ID unique ist, d.h. nicht durch einfaches „hochzählen“ der ID eine fremde Session übernommen werden kann?			
Ist der Prozess zur Kennwortwiederherstellung geregelt? • Wird bei Rücksetzung eines Kennwortes wieder ein Einmalkennwort, eine M-Tan oder eine sonstige erhöhte Sicherheitsstufe genutzt?			
Analyse von Nutzerdaten			
Ist sichergestellt, dass die Browserdaten der Webseitenbesucher nicht ausgewertet werden?			
Wird auf das Auslesen der Verlaufsdaten der Browsersitzung verzichtet?			

Zum Text

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.

ADV-Arbeitsgemeinschaft der Prüfdienste
nach § 274 SGB V
Geschäftsstelle im Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen

Eine Einrichtung der Prüfdienste der Länder und des Bundesversicherungsamtes

Verfasser:
Christian Hamsch
Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, Referat 414
Fürstenwall 25, 40219 Düsseldorf
Tel.: (0211) 8618 – 3261
Tel. mobil: 0174 162 215 3
eMail: christian.hamsch@mgepa.nrw.de
Internet: www.pruefdienst.nrw.de

Version 1.5 Stand: 10/2016

mit diesem Symbol gekennzeichnete Begriffe werden im Glossar im „Technischen Handbuch Internet“ erläutert.