TÜV geprüftes Onlineportal
Prüfgrundlagen Teil 1 – allgemeine Kriterien

1. Portalnutzung

1.1 Nutzerkonto

1.1.1 Anlegen, Ändern und Löschen des Nutzerkontos:

- Nutzerkonten dürfen verwendet werden.
- Bei der Erstellung des Nutzerkontos kommt der Portalbetreiber seiner Informationspflicht nach.
- Werden Nutzerkonten verwendet, müssen diese durch den Nutzer änderbar und löschbar sein.
- Bei Änderungen des Nutzerkontos durch den Portalbetreiber muss der Nutzer umgehend informiert werden.

1.1.2 Passwörter:

- Das Portal kann zur Nutzung der bereitgestellten Funktionen Passwörter vergeben oder durch den Nutzer Passwörter erstellen lassen. Zur Verwendung sicherer Passwörter muss das Portal in geeigneter Weise sicherstellen, dass die Passwortkomplexität / -sicherheit den spezifischen Sicherheitsanforderungen des Portals gerecht wird. Die Anforderungen an das Erstellen, Übertragen und Sichern von Passwörtern müssen sowohl bei portalseitiger Vergabe wie auch bei nutzererstellten Passwörtern eingehalten werden.
- Dem Portalnutzer müssen geeignete und sichere Verfahren zum Ändern von Passwörtern und zum Anfordern vergessener Passwörter bereitgestellt werden.

1.2 Ergonomie und Bedienbarkeit

- Das Portal muss den Grundsätzen der Dialoggestaltung hinsichtlich leichter Bedienbarkeit, Verständlichkeit und Hilfefunktionen entsprechen.

1.2.1 Aufgabenangemessenheit:

- Das Portal muss für den Nutzer effektiv und effizient nutzbar sein und den Nutzer bei der Erledigung seiner Aufgaben unterstützen. Die Menge der dargestellten Informationen darf den Nutzer nicht behindern.

1.2.2 Selbstbeschreibungsfähigkeit

- Das Portal muss dem Nutzer in geeigneter Weise allgemeine und zielgerichtete Hilfestellungen anbieten sowie bei Eingaben und Anfragen über den Bearbeitungsstand / Status informieren.

1.2.3 Erwartungskonformität:

- Die sprachliche Gestaltung des Portals muss in einer dem Inhalt und der Zielgruppe angemessenen, einfachen und verständlichen Form erfolgen. Wo erforderlich, sind dem Nutzer sinnvolle Rückmeldungen zu geben.
- Das Portal und die Darstellung der Dialoge müssen einheitlich gestaltet sein.

1.2.4 Lernförderlichkeit:

- Das Portal muss den Nutzer beim Erlernen der Bedienung angemessen unterstützen und eine entsprechende Einführung / Anleitung bereitstellen. Sind Eingaben erforderlich, müssen geeignete Rückmeldungen vorgesehen sein, insbesondere auch dann, wenn fehlerhafte Eingaben dazu führen, dass ein Vorgang nicht ausgeführt werden kann.

1.2.5 Steuerbarkeit:

- Das Portal muss vom Nutzer anpassbar sein und richtet sich bei der Bedienung nach der Arbeitsgeschwindigkeit des Nutzers.
- Eine Rückkehr zu einem vorherigen Arbeitsschritt muss möglich sein.

1.2.6 Fehlertoleranz:

- Das Portal muss in einer Art und Weise gestaltet sein, dass unbeabsichtigte Fehleingaben durch den Nutzer nicht zu Systemabstürzen oder undefinierten Systemzuständen im Portal führen. Das Portal muss Fehleingaben des Nutzers erkennen und sinnvoll behandeln. Hierbei sind Fehler deutlich zu kennzeichnen und Fehlermeldungen verständlich zu gestalten. Der Nutzer ist bei der Behebung der Ursache angemessen zu unterstützen.

1.2.7 Individualisierbarkeit

- Das Portal ist in Darstellung und Sprache auf die Bedürfnisse des Nutzers anpassbar.
- Die ursprüngliche Ansicht muss nach Veränderungen durch den Nutzer wiederherstellbar sein.

1.3 Interoperabilität (Darstellung und Funktionalität)

- Der Betreiber muss Angaben auf der Website bereitstellen, sollte das Portal für bestimmte Geräteklassen und Browser optimiert worden sein. Der Portalbetreiber darf Einschränkungen hinsichtlich der Darstellung und Nutzbarkeit vornehmen. Diese müssen transparent dargestellt sein.
- Die Darstellung und Funktionalität des Portals muss für verschiedene Geräteklassen und Browser gewährleistet sein und darf sich dabei nicht wesentlich unterscheiden oder funktional eingeschränkt sein.

1.4 Aufklärung des Nutzers bzgl. Sicherheit

- Dem Nutzer müssen Hinweise und Informationen zum Umgang mit schützenswerten Daten gegeben werden.

1.5 Sichere Nutzung des Portals

- Sollte bei der Nutzung des Portals eine Anmeldung / Login der Nutzer erforderlich sein, muss der Nutzer in Abhängigkeit der Sicherheitsanforderungen nach einer angemessenen Zeit der Inaktivität automatisiert abgemeldet werden.

1.6 Allgemeine Informationspflichten

- Informationen zum Online-Portal müssen einfach auffindbar und transparent dargestellt sein.

1.6.1 Anbieterkennzeichnung:

- Ein vollständiges Impressum muss im Portal leicht erkennbar, unmittelbar erreichbar und ständig verfügbar vorgehalten werden und die notwendigen Informationen enthalten.

1.6.2 Allgemeine Geschäftsbedingungen (AGB)/Nutzungsbedingungen:

- Die AGB/Nutzungsbedingungen müssen bei Ansprache der Verbraucher mindestens auch in deutscher Sprache zur Verfügung gestellt werden.
- Die AGB/Nutzungsbedingungen müssen leicht erkennbar und unmittelbar erreichbar in wiedergabefähiger Form, speicherbar und ausdruckbar, zur Verfügung gestellt werden.
- Diese sind mit Versionsstand und Datum zu kennzeichnen.
- Bei einem Vertragsschluss muss der Nutzer den AGB ausdrücklich zustimmen.

1.6.3 Informationen zum Datenschutz:

- Der Nutzer muss im Online-Portal einfach auffindbar umfangreiche Informationen zum Datenschutz erhalten.

1.7 Tracking-Dienste & Cookies

- Die Nutzung von Tracking-Diensten und Cookies ist zulässig.
- Wenn Tracking-, Analyse- und Statistikdienste eingesetzt werden, die personenbezogene Daten erheben, verarbeiten oder nutzen, muss der Portalbetreiber eine entsprechende Information in den Datenschutzhinweisen hinterlegen. Ein Widerspruch muss möglich sein.
- Werden Cookies eingesetzt, muss der Nutzer grundsätzlich hierüber informiert werden. Dies beinhaltet auch die Folgen für die Nutzung des Portals bei der Ablehnung von Cookies sowie die allgemeinen Risiken bei deren Verwendung. Personenbezogene Daten und Login-Informationen dürfen nicht im Klartext gespeichert werden.

1.8 Rückmeldung / Kommunikation durch den Nutzer

- Dem Nutzer muss die Möglichkeit der Kontaktaufnahme zum Portalbetreiber gegeben werden.

1.9 Datenschutzorganisation

- Der Portalbetreiber muss die anwendbaren Vorgaben zum Datenschutz ermitteln und geeignete Maßnahmen zur Einhaltung ableiten. Hierzu muss er eine angemessene und wirksame Datenschutzorganisation implementieren und aufrechterhalten.

1.9.1 Bestellung eines Datenschutzbeauftragten:

- Sofern erforderlich, muss ein Datenschutzbeauftragter schriftlich bestellt sein und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Dieser muss der Geschäftsführung direkt unterstellt und in Ausübung seiner Tätigkeit weisungsfrei sein.

1.9.2 Öffentliches Verfahrensverzeichnis:

- Der Portalbetreiber hat ein Öffentliches Verfahrensverzeichnis mit den Angaben nach § 4e Satz 1 Nr. 1 bis 8 BDSG erstellt und stellt dieses auf Anfrage Jedermann zur Verfügung.

1.9.3 Betroffenenanfragen:

- Der Portalbetreiber muss einen Prozess zum Umgang mit Betroffenenanfragen (i.S.d. BDSG) definieren und wirkungsvoll umsetzen.

2. Anforderungen an eine sichere Datenübertragung

- Der Portalbetreiber muss sicherstellen, dass die Datenübertragung nach dem Stand der Technik verschlüsselt vorgenommen wird.

2.1 Eingesetzte Protokolle

- Die eingesetzten Protokolle zur SSL/TLS Verschlüsselung müssen dem Stand der Technik entsprechen.

2.2 Angebotene Cipher Suites

- Cipher-Suites müssen dem Stand der Technik entsprechen.

2.3 Certification Authority

- Die eingesetzten Zertifikate müssen auf eine vertrauenswürdige Zertifizierungsstelle zurückgeführt werden können.
- Die Zertifikate müssen mit einem dem Stand der Technik entsprechenden Algorithmus signiert sein.

3. IT-Systeme

3.1 Technische und Organisatorische Anforderungen

- Der Portalbetreiber muss eine umfassende und aktuelle Dokumentation der eingesetzten IT-Systeme vorhalten. Es muss ein Konzept zum technischen und organisatorischen Schutz der IT-Infrastruktur gegen unbefugten Zugang und Manipulation erstellt worden sein, das den Schutzanforderungen gerecht wird und Anwendung findet.

3.2 Monitoring

- Der Portalbetreiber muss geeignete Maßnahmen zur Systemüberwachung treffen.

3.3 Updates

- Die IT-Infrastruktur ist regelmäßig zu warten und zu aktualisieren. Der Portalbetreiber muss einen Prozess definieren und wirksam umgesetzt haben, um kritische Schwachstellen zu identifizieren und unverzüglich zu behandeln.

3.4 Firewall

- Eine geeignete Firewall muss vorhanden sein und aktiv verwaltet werden.

3.5 Virenschutz

- Der Portalbetreiber muss sicherstellen, dass ein geeigneter Virenschutz vorhanden ist und regelmäßig aktualisiert wird.

3.6 Netzwerkschutz

- Es sind geeignete Maßnahmen zum Netzwerkschutz zu ergreifen.
- Ein ausfallsicherer Betrieb von kritischen Komponenten ist umzusetzen.

3.7 Rechte und Rollen

- Ein Rechte- und Rollenkonzept muss umgesetzt und regelmäßig überprüft werden.
- Dabei sind die Rechtevergabe und deren Entzug zu dokumentieren.
- Alle Benutzerkonten müssen personenbezogen benannt sein.

3.8 Backup und Restore

- Backups sind regelmäßig zu erstellen und zu überprüfen.
- Die Backupmedien sind gegen Fremdzugriff zu schützen und getrennt vom Produktivsystem zu lagern.
- Eine Wiederherstellung von Daten muss regelmäßig geprüft werden und protokolliert erfolgen.

3.9 Rechenzentrum

- Das Rechenzentrum muss dem Stand der Technik entsprechen und ausreichend physikalisch gesichert sein.
- Ein internes oder externes Audit der Rechenzentrumssicherheit muss durchgeführt worden sein.

3.10 Speicherung von Daten mit hohem Schutzbedarf

- Daten mit hohem Schutzbedarf sind mit Methoden nach dem Stand der Technik verschlüsselt.

3.11 Schutz gegen aktuelle Bedrohungen

- Der Portalbetreiber reagiert zeitnah auf aktuelle Sicherheitsbedrohungen.

4. Entwicklungs-, Freigabe- und Beschwerdeprozess

4.1 Grundlagen des Entwicklungsprozesses

- Die Entwicklung des Portals und deren Dokumentation folgen geregelten Prozessen.

4.2 Anforderungsmanagement

- Die Anforderungen neuer Entwicklungen oder erheblicher Änderungen am Portal sind schriftlich zu definieren. Ein Freigabeprozess ist nachzuweisen.

4.3 Test- und Freigabeverfahren

- Der Portalbetreiber muss einen Prozess zur Prüfung und Freigabe neuer Funktionen und Entwicklungen definieren und wirksam umsetzen.

4.4 Qualitätssicherung der Entwicklungsprozesse

- Der Portalbetreiber muss eine angemessene Qualitätssicherung betreiben und ausgewählte Mindestanforderungen erfüllen.

4.5 Beschwerdeprozess

- Für die Bearbeitung von Rückmeldungen / Beschwerden der Nutzer muss der Portalbetreiber einen angemessenen und wirkungsvollen Prozess beschrieben haben und diesen effektiv anwenden.

TÜV geprüftes Onlineportal

Prüfgrundlagen – Teil 2 sind branchenspezifisch, siehe separates Dokument