**Stand:** 07.05.2018

**Nutzungshinweis**:

Die Vorlage dient dazu, erwartete Inhalte aufzuzeigen. Die Formulierungen sind Vorschläge.

Es handelt sich nicht um eine Format-Vorlage!

Gelbe Felder sollen Beispiele markieren.

Textpassagen in [eckigen Klammern] sollen inklusive der eckigen Klammern passend ersetzt werden, wobei genannte Inhalte nicht abschließend zu verstehen sind, also auch erweitert werden dürfen.

ist eine Empfehlung und beinhaltet insbesondere inhaltliche[] zuersetzen



Sicherheitsgutachten

zum / über

[Produkttyp(en)]

der / von

[Zulassungsnehmer]

Version: [Versionsnummer]

Stand: [Datum]

Nummer des Gutachtens: [Nummer / Kürzel] [Hinweis: interne Nummerierung des Gutachters]

Erstgutachter: [Name, Firma]

Zweitgutachter: [Name, Firma]

Status: [bspw. freigegeben]

Klassifizierung: [bspw. vertraulich]

**Sicherheitsgutachter**

An der vorliegenden Version des Sicherheitsgutachtens waren beteiligt:

|  |  |
| --- | --- |
| Erstgutachter: |  |
| Name: E-Mail:Telefon:Adresse: |  |

|  |  |
| --- | --- |
| Zweitgutachter: |  |
| Name: E-Mail:Telefon:Adresse: |  |

[Bzw. erfolgt hier die Begründung, warum nur ein Sicherheitsgutachter beteiligt war, wie dies bei kleineren Delta-Gutachten der Fall sein kann.]

**Dokumentenhistorie**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Änderung | Autor |
| … | … | … | .. |
|  |  |  |  |
|  |  |  |  |

**Inhaltsverzeichnis**

[1 Zusammenfassung / Management Summary 4](#_Toc444589426)

[1.1 Aufgabenstellung 4](#_Toc444589427)

[1.2 Zusammenfassung der wesentlichen Feststellungen 4](#_Toc444589428)

[1.3 Zusammenfassung der Prüfergebnisse (inkl. Votum) 4](#_Toc444589429)

[2 Grundlagen der Prüfung 4](#_Toc444589430)

[2.1 Prüfauftrag 4](#_Toc444589431)

[2.2 Bezeichnung des Prüfobjektes 4](#_Toc444589432)

[2.3 Zielsetzung und Umfang der Prüfung 4](#_Toc444589433)

[2.4 Zeitraum der Prüfung 4](#_Toc444589434)

[3 Detaillierte Beschreibung der Prüfung 4](#_Toc444589435)

[3.1 Beschreibung des Prüfobjektes 4](#_Toc444589436)

[3.2 Beschreibung des Prüfplans 5](#_Toc444589437)

[3.3 Beschreibung der angewendeten Prüfmethoden und der durchgeführten Prüfaktivitäten 5](#_Toc444589438)

[3.3.1 Aktenanalyse 5](#_Toc444589439)

[3.3.2 Inaugenscheinnahme und Beobachtung 5](#_Toc444589440)

[3.3.3 Technische Prüfung 5](#_Toc444589441)

[3.3.4 Datenanalyse 5](#_Toc444589442)

[3.3.5 Verwendung bestehender Sicherheitsgutachten 5](#_Toc444589443)

[3.3.6 Befragung 5](#_Toc444589444)

[3.4 Beschreibung der verwendeten Prüfhilfsmittel und –tools 6](#_Toc444589445)

[3.5 Beschreibung bei Vor-Ort-Prüfungen 6](#_Toc444589446)

[3.6 Verzeichnis der Teilnehmer an der Prüfung differenziert nach 6](#_Toc444589447)

[3.7 Prüfergebnisse 7](#_Toc444589448)

[3.8 Notwendige Folgemaßnahmen und Auflagen 8](#_Toc444589449)

[4 Zusammenfassung der Prüfergebnisse 8](#_Toc444589450)

[5 Prüfungsurteil 8](#_Toc444589451)

[6 Anhang 8](#_Toc444589452)

1. Zusammenfassung / Management Summary
	1. Aufgabenstellung

[Kurze zusammenfassende Vorstellung von Zulassungsnehmer und Gutachter (als juristische Personen) sowie des Prüfobjekts.

Falls es sich um ein Delta-Gutachten mit verringertem Prüfumfang handelt, sollte dies bereits hier kurz deutlich gemacht werden.]

* 1. Zusammenfassung der wesentlichen Feststellungen

[Wie ist das Gesamtniveau hinsichtlich Datenschutz und Informationssicherheit? Sind alle Anforderungen erfüllt? Gibt es Abweichungen? Welche Auflagen wurden erteilt?]

* 1. Zusammenfassung der Prüfergebnisse (inkl. Votum)

[Votum, ggf. in Kurzform

Es muss deutlich werden, ob es sich um eine vollständige Begutachtung handelt und somit eine Sicherheitsaussage für das gesamte Prüfobjekt für die nächsten 3 Jahre getätigt wird, oder ob ein Delta-Gutachten durchgeführt wurde und somit nur ein Teil des Prüfobjekts von der Sicherheitsaussage abgedeckt ist. In letzterem Fall hat die Bestätigung des Gutachtens dann entsprechend nur eine Laufzeit bis zum Ende der Gültigkeit des Original-Gutachtens.]

1. Grundlagen der Prüfung
	1. Prüfauftrag

[Beschreibung wann, wer, wem, welchen Prüfauftrag gegeben hat]

* 1. Bezeichnung des Prüfobjektes

[Aufzählung der begutachteten Produkttypen / Prozesse]

* 1. Zeitraum der Prüfung

[In welchem Zeitraum wurde die Prüfung durchgeführt? Hierbei wird lediglich der Zeitraum der durchgeführten Prüfaktivitäten betrachtet und nicht ein sich ggf. anschließender zeitlicher Abschnitt für die Zusammenfassung aller Ergebnisse in Form des Sicherheitsgutachtens. Die Auflistung einzelne Aktivitäten erfolgt in der Beschreibung des Prüfplans.]

1. Detaillierte Beschreibung der Prüfung
	1. Beschreibung des Prüfobjektes

[Es ist das Prüfungsobjekt so kurz wie möglich aber so detailliert wie nötig zu beschreiben. Insbesondere bei Beteiligung des Prüfobjekts in einem Gesamtprozess (bspw. Kartenherausgabe) ist zu erläutern, welche Teilprozesse vom Prüfgegenstand erfüllt werden, aber auch welche explizit nicht. Für die Prüfung des Gutachtens durch die gematik muss deutlich werden, wer welche Daten von wem empfängt bzw. an wen sendet, wie die Daten geschützt sind und wer an welcher Stelle für den Schutz dieser Daten verantwortlich ist. Wenn das begutachtete Produkt den Schutz von Daten an bestimmten Stellen nicht verantwortet, ist dies hier deutlich zu machen und zu begründen.

Nur so ist ein reibungsloses Nachvollziehen der Bewertungen im Sicherheitsgutachten durch die gematik möglich (insbesondere auch das Nachvollziehen von „entbehrlichen“ Anforderungen).

Bei komplexeren Gesamtprozessen kann auch ein Schaubild hilfreich sein.

Im Falle von Delta-Gutachten ist zu beschreiben, welche Teile des Prüfobjekts begutachtet wurden.

Standorte des Auftraggebers: Es ist anzugeben, welche Standorte (*postalische Adresse jedes Standorts*) das Sicherheitsgutachten umfasst. Wenn es sich um mehrere Standorte handelt, soll im Prüfplan bei der Beschreibung der Aktivitäten (3.2) und bei der Beschreibung der Vor-Ort-Prüfungen (3.5) angegeben werden, an welchem Standort / welchen Standorten die Prüfung vorgenommen wurde. Wurden hier genannte Standorte nicht explizit vor Ort begutachtet, ist anzugeben, auf welcher Basis das Votum auch auf diese Standorte übertragen werden konnte.

Angabe der Produkt- bzw. Anbietertypversion und der Version des Produkt- bzw. Anbietertypsteckbriefs.]

* 1. Beschreibung des Prüfplans

[Tabellarische Auflistung der Prüfaktivitäten]

|  |  |  |
| --- | --- | --- |
| **Zeitraum** | **Aktivität** | **Beteiligte** |
| [von – bis] | [Durchgeführte Prüfaktivitäten, geprüfte Themen / AFOs, ggf. Standort] | [mindestens beteiligte Gutachter;ggf. Ansprechpartner, Interviewpartner] |
| … | … |  |

* 1. Beschreibung der angewendeten Prüfmethoden und der durchgeführten Prüfaktivitäten

[Kurze Beschreibung wie die Prüfmethoden umgesetzt / angewendet wurden]

* + 1. Aktenanalyse
		2. Inaugenscheinnahme und Beobachtung
		3. Technische Prüfung
		4. Datenanalyse
		5. Verwendung bestehender Sicherheitsgutachten
		6. Befragung
	1. Beschreibung der verwendeten Prüfhilfsmittel und –tools

[Wenn besondere Prüfhilfsmittel eingesetzt wurden, werden diese hier beschrieben.]

* 1. Beschreibung bei Vor-Ort-Prüfungen

[Kurze Beschreibung wann, wo (welcher Standort) genau Vor-Ort-Prüfungen durchgeführt wurden sowie ggf. Beschreibung von Besonderheiten / Prüfumgebungseinflüsse]

* 1. Verzeichnis der Teilnehmer an der Prüfung differenziert nach

[Es sind alle Beteiligten in tabellarischer Form aufzulisten]

|  |  |  |
| --- | --- | --- |
| **Name(Firma)** | **Rolle / Funktion** | **Thema** |
| **Beispiel**Peter Mustermann(Musterfirma) | Informationssicherheitsbeauftragter | Informationssicherheit, ISO 27001, Notfallmanagement |
| … | … | … |
|  |  |  |

* 1. Prüfergebnisse

[Es ist tabellarisch für jede Anforderung, die dem begutachteten Produkt zugeordnet ist (Spezifikation, Produkttypsteckbrief), zu erfassen, wie diese geprüft wurde und warum sie umgesetzt / teilweise]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AFO-ID** | **Anforderung** | **Prüfmethode** | **Umsetzungsstatus** | **Sicherheitsmängel** | **Bemerkung / Empfehlung / Risiken** |
| **Beispiel**GS-A\_4980  | Umsetzung der Norm ISO/IEC 27001  | ☒Aktenanalyse ☒Inaugenscheinnahme ☐Technische Prüfung☐Datenanalyse ☒bestehendes Gutachten ☒Befragung  | ☒AFO umgesetzt☐AFO teilweise umgesetzt☐AFO nicht umgesetzt☐AFO entbehrlich | Keine | [kurze Erläuterungen, warum die AFO als umgesetzt bewertet wurde] |
| … | … | … | … | … | … |
|  |  |  |  |  |  |

* 1. Notwendige Folgemaßnahmen und Auflagen

[Notwendige Folgemaßnahmen und Auflagen zur Erfüllung der Anforderungen, bei denen nicht der Umsetzungsstatus 'Umgesetzt' erreicht worden ist. Hier sollten in der Beschreibung jeweils die konkret betroffenen Anforderungen durch ihre AFO-ID referenziert werden.]

1. Prüfungsurteil

[Prüfungsurteil in Form eines Votums in Bezug auf die Einhaltung der sicherheitstechnischen und datenschutzrelevanten Vorgaben der Telematikinfrastruktur.

Ist das Prüfobjekt sicherheitstechnisch und datenschutzrechtlich geeignet, um nach den Vorgaben der gematik Teil der Telematikinfrastruktur zu werden?

Hier muss klar herausgestellt werden, ob es um eine Aussage bezüglich des gesamten Prüfobjekts (Bestätigung für 3 Jahre) geht oder um im Falle von Delta-Gutachten um eine Aussage für einen Teil eines insgesamt größeren Prüfobjekts (Bestätigung bis Laufzeitende des Original-Gutachten des gesamten Prüfobjekts).]

**Beispiel**

Der Gutachter ist der Auffassung, dass das gesamte Prüfobjekt nach reiflicher Prüfung und Bewertung der Sachverhalten im Zeitraum vom …. bis .... ohne Auflagen die sicherheitstechnischen und datenschutzrechtlichen Vorgaben der gematik erfüllt und geeignet ist, Teil der Telematik­infrastruktur zu werden.

1. Anhang

[Der Anhang soll:

* Abkürzungsverzeichnis,
* Glossar,
* Abbildungsverzeichnis,
* Tabellenverzeichnis,
* Referenzdokumente,
* Arbeitsdokumente (Protokolle, etc.),
* Prüfplan,
* Eigenerklärung der Sicherheitsgutachter zu Unabhängigkeit und Ob­jektivität sowie
* **Kopien der gültigen Zertifikate beider Sicherheitsgutachter(innen) zur Basisqualifikation und des Erstgutachters zur Zusatzqualifikation**

enthalten.]