Um die Suche, Begutachtung und Einführung von Onlineanwendungen zu erleichtern, stellt die IHK München und Oberbayern Muster zur Verfügung.

Versionierung des Dokumentes:

Version	Datum	Bearbeiter	Änderungen	Vertraulichkeitsstatus
1.05	11.07.2023	Bernhard Kux, IHK München und Oberbayern	Erste öffentliche Version	Öffentlich

Rechtliche Hinweise zur Benutzung:

Bitte beachten Sie für die Verwendung des hier bereit gestellten Musters Folgendes:

- Das Muster wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit.
- Das Muster ist als Formulierungshilfen zu verstehen und soll nur eine Anregung bieten, wie die eigene Aktivität zur IT-Sicherheit sachgerecht gestaltet werden kann. Dies entbindet Sie jedoch nicht von der sorgfältigen eigenverantwortlichen Prüfung.
- Das Muster ist nur ein Vorschlag für eine mögliche Gestaltung. Sie können auch andere Formulierungen wählen. Vor einer Übernahme des unveränderten Inhaltes muss daher im eigenen Interesse genau überlegt werden, ob und in welchen Teilen gegebenenfalls eine Anpassung an die konkret zu gestaltende Situation erforderlich ist.
- Auf diesen Vorgang hat die Industrie- und Handelskammer keinen Einfluss und kann daher naturgemäß für die Auswirkungen auf keine Haftung übernehmen. Auch die Haftung für leichte Fahrlässigkeit ist grundsätzlich ausgeschlossen.

Um das Muster weiter zu verbessern sind wir für Anmerkungen und Verbesserungsvorschläge sehr dankbar.
Bitte schicken Sie diese an Bernhard Kux, kux@muenchen.ihk.de

---

Muster:

Bezeichnung der Onlineanwendung:

Stand der Angaben (Ort, Datum):

Bearbeitet von:

IT-Sicherheit und Datenschutz ist ein Kernkriterium bei der Auswahl von Onlineanwendungen.

Onlineanwendungen sollten bei den im folgenden Fragebogen aufgeführten Punkten

- bei den einzelnen IT-Sicherheitsaspekten die jeweilige Mindestpunktzahl erreichen und
- alle Pflichtanforderungen erfüllen.

Sollte dies nicht der Fall sein, erreicht die Onlineanwendungen nicht die Mindestanforderungen für IT-Sicherheit. Ob die Onlineanwendungen trotzdem eingesetzt wird, bedarf der gesonderten Einschätzung.

Onlineanwendung: Mindestanforderung an IT-Sicherheit

Im Folgenden sind die Auskünfte des produktanbietenden Unternehmens („Anbieter“) genutzt, um einzuschätzen, wie mit dem Thema IT-Sicherheit bei der Onlineanwendung umgehen wird.
Dies umfasst einerseits die Onlineanwendung selbst, sowie die dafür nötigen Rahmenbedingungen, die ggf. auch von Subunternehmen (Rechenzentrum, Softwareentwicklung,…) erbracht werden.

Subunternehmen, die an der Onlineanwendung mitarbeiten:

Beschreibung der Teilleistungen (soweit zutreffend)	**Informationen zum Subunternehmen und Bezug zur Onlineanwendung**	**Risikoeinschätzung: Was ist, wenn der Dienstleister länger ausfällt?**
Rechenzentrum für Hosting, Housing o. ä.		
Cloud-Dienstleister		
Softwareentwicklung		
Website-Design		
IT-Sicherheit		
Ggf. weitere Anbieter		

Angaben zur IT-Sicherheit der Onlineanwendung. Die Angaben werden mit Punkten bewertet:

IT-Sicherheitsaspekt	**Maximale Punktzahl**	**Mindestpunktzahl**	**Punktzahl laut Angaben**	**Werden die Pflicht-Maßnahmen erfüllt?**
1. Organisatorische Maßnahmen	9	3		
2. Vertraulichkeit	21	15		
3. Integrität	15	9		
4. Verfügbarkeit	33	14		
5. Belastbarkeit	15	10		entfällt
Punktsumme	93	51		

1. Organisatorische Maßnahmen des Anbieters (max. 9 Punkte):

1.1 Betreibt der Anbieter ein Informationssicherheits-Managementsystem?
(max. 3 Punkte, bitte nur eine Antwortoption wählen)
☐ 3 Punkte: ja, inklusive Zertifizierung (bitte Zertifizierung beilegen)
oder
☐ 1 Punkt: ja, aber ohne Zertifizierung, genutztes Regelwerk (BSI, ISO27001…)
oder
☐ 0 Punkte: nein

1.2 Welche Maßnahmen zur organisatorischen IT-Sicherheit werden beim Anbieter als Anbieter eingesetzt? (max. 6 Punkte)
☐ **Pflichtanforderung: Alle Mitarbeiter sind auf die Vertraulichkeit (Datengeheimnis) verpflichtet.**

☐ 1 Punkt: Mitarbeiter des Anbieters werden in Beschäftigungs- und Vertragsbedingungen auf die Einhaltung anwendbarer Richtlinien und Anweisungen mit Bezug zu Datenschutz und Informationssicherheit verpflichtet.

☐ 1 Punkt: Es gibt einen IT-Sicherheitsbeauftragte(n) oder einen gleichwertig tätigen Mitarbeiter.

☐ 1 Punkt: Die Mitarbeiter werden zu Datenschutz und IT-Sicherheit geschult.

☐ 3 Punkte: Es gibt Risikoabschätzungen bzgl. der Abhängigkeit von Subdienstleistern (z. B. hinsichtlich Alternativen zu Subdienstleistern, Auswirkungen beim (Teil-)Ausfall eines Subdienstleisters… - siehe Liste Subdienstleister).

2. Vertraulichkeit (max. 21 Punkte)

2.1 Zutrittskontrolle Rechenzentrum (max. 4 Punkte)

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Hier: Ort, an dem die Live-Onlineanwendung technisch läuft (i.d.R. Rechenzentrum). Nicht gemeint ist die „Büroinfrastruktur“ von Anbieter oder andere Subdienstleister.

In welchen Räumlichkeiten ist die für die Onlineanwendung nötige IT untergebracht?
☐ 4 Punkte: Hosting / Housing in einem Rechenzentrum / Cloud bei einem dafür spezialisierten Anbieter siehe Liste Subunternehmer) mit professionellen Rechenzentrumsregeln (oder in firmeneigenen Räumlichkeiten, die einem professionellen Rechenzentrum gleichwertig sind).

2.2 Zugangskontrolle zur Onlineanwendung (max. 11 Punkte)

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
Hier: Wie ist die i.d.R. in einem Rechenzentrum liegende Hard- und Software für die Onlineanwendung hinsichtlich des Zugangs geschützt (üblicherweise über Logins, die für alle beteiligten Unternehmen gleich gestaltet sind).

☐ 1 Punkt: Komplexität der Passwörter (für normale Nutzer wie für Admins): Mindestens 10 Zeichen, mind. 1 Groß- & 1 Kleinbuchstaben, mind. 1 Ziffer, mind. 1 Sonderzeichen.

☐ 6 Punkte: Einsatz von Zwei-Faktor-Authentifizierung beim Admin- und Backend-Login.

☐ 4 Punkte: Logging der Login-Aktivitäten für mind. 90 Tage und Maßnahmen bei ungewöhnlichen Aktivitäten (z. B. Captcha, Sperren der Logins bei mehrfachen Fehlversuchen…).

2.3 Zugriffskontrolle auf die IT im Büro des Anbieters (max. 3 Punkte)

Maßnahmen, die 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.
Hier ist die vom Anbieter betriebene Büro-IT gemeint (z. B. in dessen Büroräumen).

☐ 1 Punkt: Zugriffsrechte der Mitarbeiter werden durch ein Berechtigungssystem geregelt.

☐ 2 Punkte: Die Anzahl und Rechte der Administratoren auf das "Notwendigste" reduziert.

2.4 Trennungskontrolle (max. 3 Punkte)

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Hier: Wie gut trennt die Onlineanwendung die eigenen Daten von fremden Daten?

☐ 2 Punkte: Die Onlineanwendung inkl. deren Daten ist abgekapselt und enthält keine Daten anderer Onlineanwendungen.

☐ 1 Punkt: Innerhalb der Onlineanwendung werden Daten so verarbeitet, dass sie getrennt für unterschiedliche Zwecke abgespeichert und verarbeitet werden.

2.5 Verschlüsselung

Die Verarbeitung (insbes. personenbezogener) Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

☐ **Pflichtanforderung: Das Onlineangebot muss mittels https nach dem Stand der Technik abgerufen werden.**

- **Es werden nur aktuelle Zertifikate und Verschlüsselungsverfahren eingesetzt,**
- **unsichere und veraltete Cipher Suites werden nicht eingesetzt.**

☐ **Pflichtanforderung: Für den Zugriff des Anbieters und seiner Subdienstleister auf das System der Onlineanwendung kommen durchgehend Verschlüsselungsverfahren zum Einsatz (z. B. VPN, SSH, sFTP etc.).**

3. Integrität (max. 15 Punkte)

3.1 Weitergabekontrolle (max. 2 Punkte)

Maßnahmen, die gewährleisten, dass (insbes. personenbezogene) Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

☐ 2 Punkte: Absicherung des Anbieter-Netzwerkes (z. B. durch Firewalls, Netzwerkseparation) nach dem Stand der Technik, wobei die Komponenten regelmäßig aktualisiert werden.

3.2 Eingabekontrolle/Verarbeitungskontrolle (max. 9 Punkte)

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in der Onlineanwendung eingegeben, verändert oder entfernt worden sind.

☐ 3 Punkte: Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten (z. B. durch Logging von Aktivitäten)

Dauer der Aufbewahrung von Logfiles der betroffenen Serverkomponenten (z. B. Betriebssystem, Webserver), die im Notfall forensisch relevant sind über (max. 6 Punkte, bitte nur eine Antwortoption wählen)

☐ 6 Punkte: mind. 6 Monate

oder

☐ 3 Punkte: mind. 3 Monate

oder

☐ 0 Punkte: weniger als 3 Monate

3.3 Dokumentationskontrolle (max. 4 Punkte)

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung (insbes. personenbezogener) Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

☐ 1 Punkt: Führung eines Verzeichnisses von Verarbeitungstätigkeiten

☐ 3 Punkte: Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

3.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass (insbes. Personenbezogene) Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

☐ **Pflichtanforderung: Es wird mit dem Auftraggeber ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen.**

☐ **Pflichtanforderung: Der Anbieter ist damit einverstanden, dass eine Kontrolle der Vertragsausführung erfolgt.**

☐ **Pflichtanforderung: Der Anbieter kann sicherstellen, dass nach Beendigung des Auftrags die Daten datenschutzkonform gelöscht werden können.**

4. Verfügbarkeit (max. 33 Punkte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

4.1. Maßnahmen im Rechenzentrum (max. 5 Punkte)

Ausfallsicherheit des Rechenzentrums, in dem die Onlineanwendung läuft über (max. 5 Punkte, bitte nur eine Antwortoption wählen):
☐ 0 Punkte: keine Redundanz, max. Ausfallzeit/Jahr über 1 Tag
oder
☐ 1 Punkt: redundanten Komponenten, max. Ausfallzeit/Jahr unter 1Tag
oder
☐ 3 Punkte: mehrfache Versorgungswege, max. Ausfallzeit/Jahr wenige Stunden
oder
☐ 5 Punkte: fehlertolerante Infrastruktur, max. Ausfallzeit/Jahr ca. 30 Min

4.2. Maßnahmen für die Sicherheit der Onlineanwendung (12 Punkte)

☐ **Pflichtanforderung: Es werden Technologien nach dem Stand der Technik eingesetzt. Bitte eingesetzte Betriebssysteme, Virtualisierungen, Datenbanken, Programmiersprachen etc. mit deren Version in einer Anlage benennen.**

☐ **Pflichtanforderung: Software-Updates werden nach einem definierten Prozess getestet und regelmäßig eingespielt, um den Stand der Technik zu erreichen,
Datum des letzten Updates bitte in einer Anlage benennen.**

☐ **Pflichtanforderung: Isolierte Backups der Onlineanwendung inkl. Daten werden erstellt und regelmäßig getestet. Bitte Backupstrategie in einer Anlage ausführen.**

☐ 1 Punkt: Bei der Softwareentwicklung der Onlineanwendung sind Verfahren zur Versionskontrolle im Einsatz (z. B. git), die Änderungen nachvollziehbar und ggf. zurücksetzbar machen.

☐ 7 Punkte: Die Onlineanwendung wird regelmäßig durch unabhängige Experten (z. B. Penetrationstests) ohne kritische Mängel getestet.
Datum des letzten Tests in einer Anlage benennen.

☐ 4 Punkte: Der Anbieter verfügt über Kenntnisse und Handlungseinschätzungen bzgl. des Standes aktueller Schwachstellen und Gefährdungen (z. B. OWASP, Common Vulnerabilities and Exposures…), die für die Onlineanwendung relevant sind. Schwachstellen und Gefährdungen werden innerhalb eines definierten Zeitraumes behoben.
Eingehaltenen Zeitraum hierzu in Tagen bitte in einer Anlage benennen.

4.3 Prozesse zum Umgang mit Schwachstellen, Sicherheitsvorfällen, Störungen (12 Punkte)

☐ **Pflichtanforderung: Anwender werden sehr zeitnah (max. 48 Stunden) über schwere Sicherheitsvorfälle informiert**

☐ 1 Punkt: Eine Richtlinie gibt Vorgaben zur Klassifizierung, Priorisierung und Eskalation von Sicherheitsvorfällen.

☐ 3 Punkte: Es ist qualifiziertes Personal (ggf. über Subunternehmen) verfügbar, das Sicherheitsvorfälle priorisieren und Sofortmaßnahmen ergreifen kann.

☐ 3 Punkte: Der Anbieter stellt Informationen und Empfehlungen für die sichere Nutzung der Onlineanwendung zur Verfügung (z. B. Handbuch / Onlinedokumentation).

☐ 5 Punkte: Es existiert ein regelmäßig aktualisierter IT-Notfallplan, der hilft, im IT-Notfall den Geschäftsbetrieb aufrecht zu erhalten und wiederherzustellen.

4.4. Maßnahmen im Büro des Anbieters (4 Punkte)

☐ **Pflichtanforderung: Backups und Testen der allgemeinen Anbieter-IT.**

☐ **Pflichtanforderung: Einsatz von Standard-Sicherheits-IT nach dem Stand der Technik mit beständiger Aktualisierung (z. B. zum Schutz vor Schadprogrammen mittels Virenabwehr, E-Mailspamfilter, Firewalls, Netzwerksegmentierung…).
Bitte in einer Anlage ausführen.**

☐ 2 Punkte: Einsatz von Systemen zur Angriffserkennung (Intrusion Detection System) auf das Firmennetzwerk.

☐ 2 Punkte: Einsatz von Sicherheitssoftware, so dass nur explizit freigegebene Anwendungen ausgeführt werden können (Anwendungs-Whitelistening z. B. Microsoft-Windows AppLocker).

5. Belastbarkeit: Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten (max. 15 Punkte)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

☐ 5 Punkte: Redundante Systemauslegung: z. B. Bereitstellung des Dienstes erfolgt aus zwei Standorten oder Cloud-Availability-Zones, die sich einander Redundanz geben.

☐ 5 Punkte: Es besteht ein getestetes Ausfallsicherheitskonzept.
Bitte in einer Anlage ausführen.

☐ 5 Punkte: Schutz vor Überlast und Denial of Service-Angriffen.