



WITTENSTEIN

Lieferantenfragebogen Informationssicherheit *Supplier Questionnaire Information Security*

1. Allgemeine Angaben / *General information*

Unternehmen und Anschrift / *Company and address*

Ansprechpartner (inkl. Kontaktdaten) / *Contact person (incl. contact details)*

Beschreibung der bereitgestellten Dienstleistungen oder Produkte / *Description of the services or products provided*

2. Informationssicherheitsmanagement *Information Security Management*

Besteht bereits eine Zertifizierung nach ISO 27001? / *Is there already an ISO 27001 certification?*

☐ Ja / Yes ☐ Nein / No

Wenn Ja, muss der Fragebogen nicht weiter ausgefüllt werden, bitte Zertifikat zusenden.
If yes, the questionnaire does not need to be filled out further, please send the certificate.

Name des Informationssicherheitsbeauftragten / *Name of Information Security Officer*

Verfügen Sie über ein zertifiziertes ISMS nach ISO 27001 oder vergleichbaren Standards? / *Do you have a certified ISMS according to ISO 27001 or comparable standards?*

☐ Ja / Yes ☐ Nein / No



WITTENSTEIN

Haben Sie Sicherheitsrichtlinien, die alle Mitarbeitenden einhalten müssen? / Do you have safety guidelines that all employees must follow?

☐ Ja / Yes ☐ Nein / No

Wie werden diese Richtlinien geschult und durchgesetzt? / How are these policies trained and enforced?

3. Technische und organisatorische Maßnahmen ***Technical and organizational measures***

Welche Maßnahmen haben Sie implementiert, um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten? / What measures have you implemented to ensure confidentiality, integrity, and availability of data

Beispiele: Firewalls, Intrusion Detection/Prevention Systems, Datenverschlüsselung /
Examples: Firewalls, Intrusion Detection/Prevention Systems, Data Encryption

Wie wird der Zugang zu Ihren IT-Systemen geregelt? Nutzen Sie ein Rollen- und Berechtigungskonzept? / How is access to your IT systems regulated? Do you use a role and authorization concept?



WITTENSTEIN

Wie oft führen Sie Sicherheitsüberprüfungen und Penetrationstests durch? / How often do you conduct security audits and penetration tests?

4. Datenschutz / Privacy

Sind Sie konform mit der DSGVO (falls zutreffend) oder anderen relevanten Datenschutzgesetzen? Are you compliant with the GDPR (if applicable) or other relevant data protection laws?

☐ Ja / Yes ☐ Nein / No

Wie werden personenbezogene Daten geschützt und verarbeitet? / How is personal data protected and processed?

Gibt es Regelungen zum Schutz von Informationen bei der Verarbeitung durch Dritte oder Subdienstleister? / Are there any regulations for the protection of information during processing by third parties or subcontractors?

☐ Ja / Yes ☐ Nein / No

5. Notfallmanagement / Emergency management

Verfügen Sie über ein dokumentiertes Notfall- und Krisenmanagement? / Do you have documented emergency and crisis management?

☐ Ja / Yes ☐ Nein / No

Gibt es Prozesse für die regelmäßige Überprüfung und Aktualisierung Ihrer Notfallpläne? Are there processes in place for regularly reviewing and updating your emergency plans?

☐ Ja / Yes ☐ Nein / No



WITTENSTEIN

Wie wird die Verfügbarkeit Ihrer Systeme und Dienstleistungen im Notfall sichergestellt? / How is the availability of your systems and services ensured in the event of an emergency?

6. Compliance und rechtliche Anforderungen / Compliance and legal requirements

Wie stellen Sie sicher, dass Sie gesetzliche und regulatorische Vorgaben einhalten? / How do you ensure that you comply with legal and regulatory requirements?

Haben Sie Prozesse zur Erkennung und Meldung von Sicherheitsvorfällen? / Do you have processes in place to detect and report security incidents?

☐ Ja / Yes ☐ Nein / No

7. Audit und Berichterstattung / Audit and reporting

Erlauben Sie Ihren Kunden, Audits Ihrer Sicherheitsmaßnahmen durchzuführen? / Do you allow your customers to conduct audits of your security measures?

☐ Ja / Yes ☐ Nein / No

Welche Berichte oder Nachweise können Sie zur Verfügung stellen, um die Einhaltung von Sicherheitsstandards zu belegen? / What reports or evidence can you provide to demonstrate compliance with safety standards?



WITTENSTEIN

8. Subunternehmen und Drittanbieter / *Subcontractors and Third-Party Providers*

Nutzen Sie Subunternehmen oder Drittanbieter für die Erbringung Ihrer Dienstleistungen? / *Do you use subcontractors or third-party service providers to provide your services?*

☐ Ja / Yes ☐ Nein / No

Wenn ja: Wie stellen Sie sicher, dass diese ebenfalls die Sicherheitsanforderungen einhalten? / *If so, how do you ensure that they also comply with the safety requirements?*

Wenn ja: Gibt es Verträge mit Sicherheitsvorgaben? / *If so, are there contracts with security requirements?*

☐ Ja / Yes ☐ Nein / No

9. Abschließende Fragen / *Final Questions*

Welche weiteren Zertifizierungen oder Standards erfüllen Sie? (z. B. ISO 9001, TISAX)? / *What other certifications or standards do you meet? (e.g. B. ISO 9001, TISAX)?*

Gibt es aktuelle Sicherheitsvorfälle oder Verstöße gegen Datenschutzgesetze, über die wir informiert werden sollten? / *Are there any current security incidents or violations of data protection laws that we should be informed about?*