NIS 2 ART. 21(2)(D)

NIS 2 Lieferantenfragebogen

Offener Fragebogen für die Lieferantenbewertung unter NIS 2, im EU-Recht verankert

Lieferantenprofil	16 Felder
Sicherheitspraktiken	31 Felder
Software als Dienst (SaaS)	2 Felder
Software beim Kunden (On-Premise)	4 Felder

Jede Frage nennt ihre Quelle auf EU-Ebene: die Durchführungsverordnung (EU) 2024/2690, die ENISA Technical Implementation Guidance, die DSGVO oder den Cyber Resilience Act. Dient sie Maßnahmen aus Anhang A der ISO/IEC 27001:2022, stehen diese daneben. 21 Fragen beantwortet jeder Lieferant; bei jeder weiteren steht, unter welcher Antwort sie gestellt wird. Das hängt davon ab, was der Lieferant bei seinen Kunden erreicht: ihre Daten, ihre Systeme, ihre Räume oder Software, die er betreibt oder ausliefert. Sektorspezifische Erweiterungen (TISAX, VDA ISA, BSI C5, KRITIS) ergänzen die Basis, ersetzen sie nicht.

Quelle: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

Lizenz: MIT (Schema) + CC BY 4.0 (Inhalt). Frei nutzbar, forkbar, anpassbar.

1. Lieferantenprofil

16 Felder

Firmierung (Rechtsname)

STRING · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2

Der eingetragene Name Ihres Unternehmens, so wie er im Handelsregister steht. Beispiel: Müller GmbH oder Schmidt AG.

Geschäftsanschrift

STRING · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2

Die Geschäftsanschrift Ihres Unternehmens. Eine Adresse genügt, auch wenn Sie mehrere Standorte haben.

Land

COUNTRY · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2

Das Land, in dem Ihr Unternehmen rechtlich sitzt. Zwei Buchstaben, zum Beispiel DE für Deutschland.

Primäre Domain

DOMAIN · OPTIONAL · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(A)

Ihre Hauptdomain, üblicherweise die Adresse Ihrer Webseite. Beispiel: muellergmbh.de.

Beschreibung der erbrachten Leistungen

TEXT · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Ein Absatz dazu, was Sie Kunden liefern: konkrete Produkte, Dienste oder Arbeiten, keine Werbung. Beispiele: „Büroreinigung an drei Abenden pro Woche, mit Schlüssel zum Gebäude“ oder „Lohnabrechnung für bis zu 200 Mitarbeitende“.

Name des Sicherheitskontakts

STRING · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

Wer bei einem Sicherheitsvorfall direkt angesprochen wird. Bei kleineren Unternehmen oft die Geschäftsführung oder die IT-Leitung. Eine Person genügt.

E-Mail für Vorfälle

EMAIL · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

E-Mail-Adresse, die Kunden bei einem Sicherheitsvorfall verwenden. Idealerweise ein Verteiler wie security@firma.de, der mehrere Personen erreicht.

Telefonnummer für Vorfälle

PHONE · OPTIONAL · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(A) · ISO/IEC 27001:2022 A.5.20, A.5.24

Telefonnummer für dringende Vorfallsmeldungen. Nennen Sie in Klammern, wann sie besetzt ist; eine Erreichbarkeit rund um die Uhr wird nicht erwartet.

Wie schnell Sie Kunden über einen Vorfall informieren (Stunden)

INTEGER · OPTIONAL · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(D) · ISO/IEC 27001:2022 A.5.20, A.5.24

Höchstens so viele Stunden, nachdem Sie einen Sicherheitsvorfall bemerkt haben, der einen Kunden betrifft, zum Beispiel ein Datenleck, ein gehacktes Konto oder einen verlorenen Schlüssel. Ein Kunde unter NIS 2 muss seiner Behörde einen erheblichen Sicherheitsvorfall innerhalb von 24 Stunden, nachdem er davon erfahren hat, als Frühwarnung melden (Art. 23 Abs. 4 Buchst. a NIS 2). Eine Zusage von 24 Stunden oder weniger hilft ihm deshalb am meisten. Nennen Sie einen Wert, den Sie halten.

Wir bieten SaaS / gehostete Dienste

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22, A.5.23

Sie betreiben Software für Kunden auf eigener Infrastruktur und liefern sie über das Internet. Mehrfachauswahl möglich, wenn Sie mehrere Modelle anbieten.

Wir liefern On-Prem-Software

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Sie liefern Software, die Ihre Kunden auf ihrer eigenen Infrastruktur installieren und betreiben.

Wir bieten Managed Services / MSP

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.2(B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Sie betreiben Teile der IT-Landschaft des Kunden für ihn, mit eigenem Personal. Typisch für MSP- und MSSP-Modelle.

Wir verarbeiten oder speichern Daten unserer Kunden

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19

Ja, wenn Sie Daten oder Unterlagen Ihrer Kunden elektronisch oder auf Papier halten oder bearbeiten, etwa in Software, Rechenzentrum, Ticketsystem, Buchhaltung oder Archiv.

Länder / Regionen, in denen Kundendaten verarbeitet werden

STRING · BEDINGT · RECHTSGRUNDLAGE: ENISA TIG §5.1.4 TIPS · ISO/IEC 27001:2022 A.5.20, A.5.23, A.5.34

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja

Alle Länder, in denen Kundendaten Ihrer Kunden gespeichert oder verarbeitet werden. Komma-getrennt, ISO-Ländercodes. Beispiel: DE, NL, US. Wenn Sie ausschließlich in der EU verarbeiten, reicht eine Liste der EU-Länder.

Wir greifen auf Systeme unserer Kunden zu

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19

Ja, wenn Sie sich bei Ihren Kunden anmelden können, aus der Ferne, als Administrator oder vor Ort, zum Beispiel für Wartung, Support oder Betrieb.

Unsere Mitarbeitenden betreten Räume unserer Kunden

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §11.1.2(A); §13.3.2(B) · ISO/IEC 27001:2022 A.5.19

Ja, wenn Ihre Mitarbeitenden oder Unterauftragnehmer Büros oder Gebäude eines Kunden betreten, mit oder ohne Begleitung, etwa für Reinigung, Wartung, Reparaturen, Anlieferung ins Gebäude oder Support vor Ort. Schlüssel, Ausweise oder Türcodes zählen dazu.

2. Sicherheitspraktiken

31 Felder

Mitarbeitende, die für Kunden arbeiten, werden zu Beginn und danach regelmäßig in Sicherheit unterwiesen

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(B) · ISO/IEC 27001:2022 A.6.3

Ja, wenn alle, die für Kunden arbeiten, die für sie geltenden Sicherheitsregeln zu Beginn und danach regelmäßig vermittelt bekommen, etwa in einer kurzen Unterweisung, einem E-Learning oder schriftlichen Regeln, die sie unterschreiben.

Wir akzeptieren Audits durch Kunden oder stellen Prüfberichte bereit

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(E) · ISO/IEC 27001:2022 A.5.20, A.5.22

Ja, wenn Sie Kunden entweder ein Auditrecht einräumen oder ihnen stattdessen Prüfberichte (zum Beispiel SOC 2, ISAE 3402) zur Verfügung stellen.

Wir setzen für unsere Leistung Unterauftragnehmer ein

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Ja, wenn andere Unternehmen an Ihrer Leistung mitwirken und dabei an Daten, Systeme oder Räume Ihrer Kunden gelangen. Beispiele: ein Cloudanbieter wie AWS oder Azure, ein Zahlungsdienst oder ein beauftragtes Team, das vor Ort arbeitet.

Liste der Unterauftragnehmer

TEXT · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Nur wenn: Wir setzen für unsere Leistung Unterauftragnehmer ein = Ja

Alle Unterauftragnehmer mit Name, Ort und Aufgabe. Eine Zeile pro Unterauftragnehmer genügt. Aktualisieren Sie die Liste, wenn Sie einen hinzufügen oder entfernen.

Wir verpflichten Unterauftragnehmer auf vergleichbare Sicherheitsanforderungen

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Nur wenn: Wir setzen für unsere Leistung Unterauftragnehmer ein = Ja

Ja, wenn Ihre Verträge mit Unterauftragnehmern Sicherheitsanforderungen enthalten, die dem entsprechen, was Ihre Kunden von Ihnen verlangen, etwa zu Vorfällen, Zugängen und dem Umgang mit Daten.

Wir informieren Kunden über wesentliche Änderungen, auch der Verarbeitungsorte

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: ENISA TIG §5.1.4 · ISO/IEC 27001:2022 A.5.22

Ja, wenn Sie Kunden vorab informieren, bevor sich an Ihrer Leistung etwas Wesentliches ändert: eine Übernahme, ein neuer Unterauftragnehmer, ein anderer Hoster oder ein neues Land, in dem ihre Daten verarbeitet werden.

Auf Anfrage informieren wir Kunden über Sicherheitsvorfälle, die Kunden betrafen

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.22

Ja, wenn Sie auf Anfrage eines Kunden offen sagen, ob und welche Sicherheitsvorfälle mit Auswirkung auf Kunden es bei Ihnen gab.

Wir liefern Kunden die Angaben, die ihre Behörde verlangt

BOOLEAN · PFLICHTFELD · RECHTSGRUNDLAGE: ENISA TIG §5.1.4 · ISO/IEC 27001:2022 A.5.20, A.5.31

Ja, wenn Sie Ihren Kunden die Angaben liefern, die deren Aufsichtsbehörde nach einem Vorfall oder bei einer Prüfung verlangt. Sofern Sie nicht selbst eine wesentliche oder wichtige Einrichtung unter NIS 2 sind, sind Sie dieser Behörde nicht selbst verpflichtet; die Pflicht hat Ihr Kunde, und Sie helfen ihm, sie zu erfüllen.

Alle, die für unsere Kunden arbeiten, sind zur Verschwiegenheit verpflichtet

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: ENISA TIG §5.1 TIPS; CIR 2024/2690 §10.3.2 · ISO/IEC 27001:2022 A.6.6

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Unsere Mitarbeitenden betreten Räume unserer Kunden = Ja

Ja, wenn alle, die für Kunden arbeiten, sich im Arbeitsvertrag oder separat schriftlich zur Verschwiegenheit verpflichtet haben oder gesetzlich zur Verschwiegenheit verpflichtet sind.

Wir prüfen die Eignung von Mitarbeitenden, die Zugang bei Kunden erhalten

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §10.2.1 · ISO/IEC 27001:2022 A.6.1

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Unsere Mitarbeitenden betreten Räume unserer Kunden = Ja

Ja, wenn Sie vor dem Einsatz prüfen, ob Mitarbeitende mit Zugang zu Daten, Systemen oder Räumen von Kunden (etwa Schlüsselinhaber) für diese Rolle geeignet sind, soweit Arbeitsrecht und Datenschutz es erlauben: etwa Referenzen oder, wo zulässig und für die Rolle nötig, ein Führungszeugnis. Eine Prüfung aller Mitarbeitenden wird nicht erwartet.

Bei Vertragsende geben wir zurück oder vernichten, was wir vom Kunden haben

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(H); §5.1.2(D) · ISO/IEC 27001:2022 A.5.11, A.8.10

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Unsere Mitarbeitenden betreten Räume unserer Kunden = Ja

Ja, wenn Ihr Vertrag Sie verpflichtet, die Daten des Kunden in einem nutzbaren, beschriebenen Format (etwa CSV oder JSON) zurückzugeben und dann zu löschen, Schlüssel, Ausweise und Unterlagen zurückzugeben und Zugänge beim Kunden zu schließen.

Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO)

ENUM · BEDINGT · RECHTSGRUNDLAGE: GDPR ART. 28(3); ART. 4(7) · ISO/IEC 27001:2022 A.5.34

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja

Nötig, wenn Sie personenbezogene Daten im Auftrag und nach Weisung eines Kunden verarbeiten (Art. 28 Abs. 3 DSGVO). Manche Berufe sind von Gesetzes wegen selbst Verantwortliche und schließen keinen ab, in Deutschland etwa Steuerberater (§ 11 Abs. 2 StBerG).

- ○ Ja, wir bieten einen Mustervertrag an
- ○ Nicht nötig: Wir sind selbst Verantwortlicher (zum Beispiel Steuerberater)
- ○ Nicht nötig: Wir verarbeiten für Kunden keine personenbezogenen Daten
- ○ Nein

Kundendaten, die wir elektronisch speichern, sind verschlüsselt

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(C); §9.2(A) · ISO/IEC 27001:2022 A.8.24

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja

Ja, wenn Kundendaten überall verschlüsselt sind, wo Sie sie elektronisch speichern: auf Servern, Laptops, Telefonen und Sicherungen, etwa mit BitLocker, FileVault oder der Festplattenverschlüsselung Ihres Cloudanbieters.

Kundendaten, die wir übertragen, sind verschlüsselt

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(C); §9.2(A) · ISO/IEC 27001:2022 A.8.24

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja

Ja, wenn Ihre Webseiten und Schnittstellen HTTPS mit TLS 1.2 oder höher nutzen und Dateien über ein verschlüsseltes Portal oder verschlüsselte E-Mail an Kunden gehen.

Wir betreiben ein dokumentiertes Informationssicherheitsmanagementsystem (ISMS)

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A) · ISO/IEC 27001:2022 A.5.1

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn Sie eine schriftliche Richtlinie zur Informationssicherheit haben, klar zugewiesene Rollen, regelmäßige Überprüfungen und einen dokumentierten Umgang mit Vorfällen. Eine Zertifizierung nach ISO/IEC 27001, auch auf Basis von IT-Grundschutz, bedeutet Ja.

Wir haben ein gültiges Sicherheitszertifikat oder einen Prüfbericht, der die Leistung für unsere Kunden abdeckt

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A); ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.19, A.5.22

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Es zählen: ISO/IEC 27001 (auch auf Basis von IT-Grundschutz), ein Testat nach BSI C5, ein Label nach TISAX, ein Bericht nach SOC 2 Typ II oder ISAE 3402 oder ein europäisches Cybersicherheitszertifikat. Ja nur, wenn der Geltungsbereich die Leistung für Ihre Kunden abdeckt.

Zertifikat oder Bericht: Standard, ausstellende Stelle, gültig bis, Geltungsbereich

TEXT · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A); ENISA TIG §5.1.2 · ISO/IEC 27001:2022 A.5.22

Nur wenn: Wir haben ein gültiges Sicherheitszertifikat oder einen Prüfbericht, der die Leistung für unsere Kunden abdeckt = Ja

Übernehmen Sie den Geltungsbereich so, wie er auf dem Zertifikat oder Bericht steht. Mehrere? Eines pro Zeile.

Wir spielen Sicherheitsupdates zeitnah ein und gehen bekannten Schwachstellen nach

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(F) · ISO/IEC 27001:2022 A.8.8

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn Sie für Sicherheitslücken in den Systemen und Programmen, die Sie für Kunden nutzen, ein festes Vorgehen haben: Sie erfahren davon, schätzen die Dringlichkeit ein und spielen das Update rechtzeitig ein oder ergreifen eine andere Maßnahme.

Wir haben einen schriftlichen Plan für Sicherheitsvorfälle

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A); §3.1 · ISO/IEC 27001:2022 A.5.24, A.5.26

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn ein schriftlicher Plan festlegt, wie Sie mit einem Sicherheitsvorfall umgehen: wer entscheidet, wer die Kunden informiert und wer dokumentiert.

Wir haben einen schriftlichen Plan für Ausfälle, einschließlich Sicherungen

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(C); §4.1; §4.2 · ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.13

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn ein schriftlicher Plan festlegt, wie Sie nach einem Ausfall weiterarbeiten oder wieder anlaufen, einschließlich Sicherungen der Daten, die Sie für Kunden halten, getrennt von den laufenden Systemen und probeweise zurückgespielt. Er nennt die wichtigen Systeme, den Ersatzweg und wie lange ein Ausfall höchstens dauern und wie viele Daten höchstens verloren gehen dürfen.

Alle internen Administratorkonten sind mit einem zweiten Faktor geschützt

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A); §11.7 · ISO/IEC 27001:2022 A.8.5, A.8.2

Nur wenn: Wir verarbeiten oder speichern Daten unserer Kunden = Ja oder Wir greifen auf Systeme unserer Kunden zu = Ja oder Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn jedes Konto mit Administratorrechten in Ihren eigenen Systemen (E-Mail, Cloud, Server, Buchhaltung) zur Anmeldung einen zweiten Faktor braucht, etwa eine App oder einen Sicherheitsschlüssel. Codes per SMS zählen, sind aber die schwächste Variante.

Die Systeme, mit denen wir Kunden bedienen, werden von einer unabhängigen Stelle auf Sicherheit getestet

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A); §6.5 · ISO/IEC 27001:2022 A.8.29, A.8.8

Nur wenn: Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja oder Wir bieten Managed Services / MSP = Ja

Ja, wenn eine unabhängige Stelle diese Systeme auf Sicherheitslücken prüft, so oft, wie es Ihr Risiko verlangt. Ein Penetrationstest und ein externer Schwachstellenscan zählen beide.

Wir entwickeln nach festgelegten Regeln für sichere Entwicklung

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(A) · ISO/IEC 27001:2022 A.8.25, A.8.28

Nur wenn: Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja

Ja, wenn Ihre Entwicklung festen Regeln folgt, zum Beispiel einer Prüfung vor jeder Änderung, die live geht, aktuellen Abhängigkeiten, Tests und einer Prüfung auf bekannte Schwachstellen. Gefragt nur bei Lieferanten, die Software als Dienst betreiben oder ausliefern.

Wir veröffentlichen, wie man uns eine Sicherheitslücke meldet

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(F); CRA ANNEX I PART II(5), (6) · ISO/IEC 27001:2022 A.8.8, A.5.21

Nur wenn: Wir bieten SaaS / gehostete Dienste = Ja oder Wir liefern On-Prem-Software = Ja

Ja, wenn auf Ihrer Webseite steht, wie man Ihnen eine Sicherheitslücke meldet und was Sie dann tun, etwa in einer security.txt (RFC 9116). Ab dem 11.12.2027 verlangt der Cyber Resilience Act diese Regelung und eine Kontaktadresse von Herstellern von Softwareprodukten.

Zugriffe auf Kundensysteme laufen über persönliche Konten mit zweitem Faktor

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(A); §11.3.2(A); §11.5.2(B) · ISO/IEC 27001:2022 A.8.2, A.8.5, A.5.16

Nur wenn: Wir greifen auf Systeme unserer Kunden zu = Ja

Ja, wenn alle, die sich bei Kunden anmelden, ein eigenes Konto mit zweitem Faktor nutzen, auch bei Fernwartung, etwa mit TeamViewer; niemand teilt sich eine Anmeldung.

Administrative Zugriffe auf Kundensysteme werden protokolliert

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(A); §3.2.3(E) · ISO/IEC 27001:2022 A.8.15

Nur wenn: Wir greifen auf Systeme unserer Kunden zu = Ja

Ja, wenn festgehalten wird, wer wann mit Administratorrechten auf Systeme Ihrer Kunden zugegriffen hat, sodass es sich später nachvollziehen lässt. Ganze Sitzungen aufzuzeichnen wird nicht erwartet.

Wir verwalten Schlüssel, Ausweise und Codes unserer Kunden nachvollziehbar

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(A); §11.2.2(D); §13.3.2(B) · ISO/IEC 27001:2022 A.7.2, A.5.11, A.5.18

Nur wenn: Unsere Mitarbeitenden betreten Räume unserer Kunden = Ja

Ja, wenn Sie jederzeit wissen, wer welchen Schlüssel, Ausweis oder Code hat, ihn bei Ausscheiden oder Aufgabenwechsel zurücknehmen und den Kunden unverzüglich informieren, wenn einer verloren geht.

Unsere Mitarbeitenden halten sich in Räumen von Kunden an schriftliche Verhaltensregeln

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: ENISA TIG §5.1 TIPS; CIR 2024/2690 §8.1.1 · ISO/IEC 27001:2022 A.7.2, A.7.7, A.6.3

Nur wenn: Unsere Mitarbeitenden betreten Räume unserer Kunden = Ja

Ja, wenn Ihre Mitarbeitenden schriftliche Regeln für die Arbeit bei Kunden haben, zum Beispiel: niemanden hereinlassen, Bildschirme, Geräte und Unterlagen nicht anfassen, Auffälliges dem Kunden melden.

Personenbezogene Daten Ihrer Kunden außerhalb des Europäischen Wirtschaftsraums

ENUM · BEDINGT · RECHTSGRUNDLAGE: GDPR ART. 44; ART. 45; ART. 46(2)(C); ART. 47

Nur wenn: Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Ja, wir bieten einen Mustervertrag an oder Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Nein

Ob Sie oder Ihre Unterauftragsverarbeiter personenbezogene Daten Ihrer Kunden in ein Land außerhalb des EWR übermitteln, und auf welcher Grundlage. Eine Übermittlung braucht eine der Grundlagen aus Kapitel V DSGVO (Art. 44).

- ○ Nein, sie bleiben im EWR
- ○ Ja, nur in Länder mit Angemessenheitsbeschluss der Europäischen Kommission (Art. 45)
- ○ Ja, auf Grundlage der Standardvertragsklauseln der Europäischen Kommission (Art. 46 Abs. 2 Buchst. c)
- ○ Ja, auf Grundlage verbindlicher interner Datenschutzvorschriften (Art. 47)
- ○ Ja, auf anderer Grundlage

Wie Sie Unterauftragsverarbeiter einsetzen

ENUM · BEDINGT · RECHTSGRUNDLAGE: GDPR ART. 28(2)

Nur wenn: Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Ja, wir bieten einen Mustervertrag an oder Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Nein

Ein Auftragsverarbeiter nimmt einen weiteren nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Kunden in Anspruch. Bei einer allgemeinen informiert er den Kunden über jede beabsichtigte Hinzunahme oder Ersetzung, damit dieser widersprechen kann (Art. 28 Abs. 2 DSGVO).

- ○ Allgemeine Genehmigung: Wir informieren Sie vor jeder Hinzunahme oder Ersetzung, und Sie können widersprechen
- ○ Wir holen für jeden einzelnen Ihre gesonderte Genehmigung ein
- ○ Wir setzen für personenbezogene Daten unserer Kunden keine Unterauftragsverarbeiter ein

Wir melden Ihnen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie uns bekannt wird

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: GDPR ART. 33(2)

Nur wenn: Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Ja, wir bieten einen Mustervertrag an oder Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO) = Nein

Das schuldet ein Auftragsverarbeiter dem Verantwortlichen (Art. 33 Abs. 2 DSGVO). Der Verantwortliche braucht die Meldung, um seine eigene Meldepflicht gegenüber der Aufsichtsbehörde zu erfüllen (Art. 33 Abs. 1).

3. Software als Dienst (SaaS)

2 Felder

Kunden können ihre Konten mit einem zweiten Faktor schützen

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.2(C); §11.7 · ISO/IEC 27001:2022 A.8.5, A.5.23

Nur wenn: Wir bieten SaaS / gehostete Dienste = Ja

Ja, wenn Ihre Anwendung eine Anmeldung mit zweitem Faktor anbietet (App, Sicherheitsschlüssel oder Einmalcode), mindestens für die Administratoren Ihrer Kunden. Ihre eigenen internen Administratorkonten fragt ein eigener Punkt unter Sicherheit im Betrieb ab.

Längste Ausfallzeit bis zur Wiederherstellung (Stunden)

INTEGER · BEDINGT · RECHTSGRUNDLAGE: ENISA TIG §5.1 TIPS · ISO/IEC 27001:2022 A.5.30, A.5.23

Nur wenn: Wir bieten SaaS / gehostete Dienste = Ja

So viele Stunden darf Ihr Dienst höchstens ausfallen, bis er wiederhergestellt ist. Nennen Sie einen Wert, den Sie halten.

4. Software beim Kunden (On-Premise)

4 Felder

Bis wann Sie für die gelieferte Version Sicherheitsupdates liefern

STRING · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §6.1.2(B); CRA ART. 13(19) · ISO/IEC 27001:2022 A.5.21

Nur wenn: Wir liefern On-Prem-Software = Ja

Monat und Jahr oder die Regel, nach der Sie gehen. Ab dem 11.12.2027 verlangt der Cyber Resilience Act, dass Hersteller dieses Datum beim Kauf angeben.

Frist für Sicherheitsupdates bei kritischen Schwachstellen (Stunden)

INTEGER · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §5.1.4(F); CRA ANNEX I PART II(2) · ISO/IEC 27001:2022 A.8.8

Nur wenn: Wir liefern On-Prem-Software = Ja

Stunden vom Bekanntwerden einer kritischen Schwachstelle bis zu Ihrem korrigierten Release. Ab dem 11.12.2027 verlangt der Cyber Resilience Act von Herstellern, Schwachstellen unverzüglich zu beheben.

Kunden erhalten auf Wunsch eine Software Bill of Materials (SBOM)

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §6.1.2(C); CRA ANNEX I PART II(1) · ISO/IEC 27001:2022 A.5.21

Nur wenn: Wir liefern On-Prem-Software = Ja

Ja, wenn Sie Kunden zu Ihren Releases eine SBOM geben (CycloneDX oder SPDX). Ab dem 11.12.2027 verlangt der Cyber Resilience Act von Herstellern eine SBOM in der technischen Dokumentation von Produkten mit digitalen Elementen; sie an Kunden weiterzugeben, steht Ihnen frei.

Releases und Updates sind signiert

BOOLEAN · BEDINGT · RECHTSGRUNDLAGE: CIR 2024/2690 §6.6.1(C); CRA ANNEX I PART II(7) · ISO/IEC 27001:2022 A.5.21

Nur wenn: Wir liefern On-Prem-Software = Ja

Ja, wenn jedes Release und jedes Update eine Signatur trägt, die Ihre Kunden vor der Installation prüfen können, zum Beispiel Sigstore, Authenticode oder PGP.