IDW PS 860

Bericht über die BSI C5-Wirksamkeitsprüfung des Cloud-Service „beesite Recruiting“

milch & zucker GmbH
Gießen
Zeitraum 1. Juni bis 31. Dezember 2025

Dr. Stückmann und Partner mbB
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Elsa-Brändström-Straße 7
33602 Bielefeld
www.stueckmann.de

HLB STÜCKMANN

INHALTSVERZEICHNIS

Abkürzungsverzeichnis 4

Prüfungsbericht des unabhängigen Wirtschaftsprüfers über die Prüfung einer Erklärung der gesetzlichen Vertreter

Erstellt durch HLB Dr. Stückmann und Partner mbB 5

Anlage 1
Erklärung der gesetzlichen Vertreter

Erstellt durch milch & zucker GmbH 10

1. Unternehmenshintergrund 11
3. Internes Kontrollsystem und BSI C5:2020 Kriterien 13
4. Hinweise zur Anwendbarkeit und Korrespondierende Kontrollen beim Dienstleistungsempfänger 13
5. Informationssicherheitsmanagement (OIS) 15
6. Sicherheitsrichtlinien und Arbeitsanweisungen (SP) 15
7. Personalsicherheit (HR) 16
8. Asset Management (AM) 16
9. Physische Sicherheit (PS) 17
10. Service Desk/ Regelbetrieb (OPS) 17
11. Zugangskontrollen und Berechtigungsmanagement (IDM) 18
12. Kryptografie, Schlüsselmanagement und Backup (CRY) 18
13. Kommunikationssicherheit (COS) 19
14. Portabilität und Interoperabilität (PI) 20
15. Beschaffung, Entwicklung und Änderungen von Informationssystemen (DEV) 20
16. Lieferantenmanagement (SSO) 21
17. Umgang mit Sicherheitsvorfällen/Störungsmanagement (SIM) 21
18. Business Continuity Management (BCM) 22
19. Compliance (COM) 22
20. Umgang mit Ermittlungsfragen staatlicher Stellen (INQ) 23
21. Produktsicherheit (PSS) 23

Anlage 2
Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse

Erstellt durch HLB Dr. Stückmann und Partner mbB 25

1. Organisation der Informationssicherheit (OIS) 26
2. Sicherheitsrichtlinien und Arbeitsanweisungen (SP) 33
3. Personal (HR) 35
4. Asset Management (AM) 40
5. Physische Sicherheit (PS) 45
6. Regelbetrieb (OPS) 53
7. Identitäts- und Berechtigungsmanagement (IDM) 69
8. Kryptographie und Schlüsselmanagement (CRY) 76
9. Kommunikationssicherheit (COS) 80
10. Portabilität und Interoperabilität (PI) 86
11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV) 88
12. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO) 97
13. Umgang mit Sicherheitsvorfällen (SIM) 103
14. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM) 106
15. Compliance (COM) 110
16. Umgang mit Ermittlungsfragen staatlicher Stellen (INQ) 113
17. Produktsicherheit (PSS) 116

Anlage 3
Allgemeine Auftragsbedingungen 126

ABKÜRZUNGSVERZEICHNIS

Abkürzung	Beschreibung
BCM	Business Continuity Management
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarisierte Zone
IdP	Identity Provider
ISMS	Informationssicherheitsmanagementsystem
LUKS	Linux Unified Key Setup
RBAC	Role-Based Access Control
TLS	Transport Layer Security
UAT	User Acceptance Test

PRÜFUNGSBERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER

ERSTELLT DURCH

HLB DR. STÜCKMANN UND PARTNER MBB

PRÜFUNGSBERICHT DES UNABHÄNGIGEN WIRTSCHAFTSPRÜFERS ÜBER DIE PRÜFUNG EINER ERKLÄRUNG DER GESETZLICHEN VERTRETER

An die gesetzlichen Vertreter der

milch & zucker GmbH, Gießen, Deutschland,
– im Folgenden kurz „milch & zucker“, „Gesellschaft” oder „Cloud-Anbieter“ –

Auftrag

Wir haben die in der Anlage 1 beigefügte Erklärung der gesetzlichen Vertreter zur Beschreibung der von der milch & zucker für das Cloud-Servicemodell „beesite Recruiting“ umzusetzenden Maßnahmen sowie die Geeignetheit und Implementierung und Wirksamkeit dieser Maßnahmen für den Zeitraum vom 1. Juni bis zum 31. Dezember 2025 mit hinreichender Sicherheit geprüft. Die Maßnahmen sind geeignet, wenn sie den Risiken der Nichterreichung der unten genannten Kriterien mit hinreichender Sicherheit begegnen.

Verantwortung der gesetzlichen Vertreter

Die gesetzlichen Vertreter der milch & zucker sind für die Aufstellung der Erklärung des Cloud-Anbieters verantwortlich. Dies schließt die Verantwortung für die internen Kontrollen ein, die sie als notwendig erachten, um eine Erklärung aufzustellen, die frei von wesentlichen - beabsichtigten und unbeabsichtigten - Fehlern ist.

Des Weiteren sind die gesetzlichen Vertreter dafür verantwortlich, dass die Maßnahmen gemäß den unten genannten Kriterien in allen wesentlichen Belangen

- so konzipiert werden, dass sie geeignet sind,
- implementiert werden und wirksam sind, d.h. auch
- überwacht und dokumentiert werden.

Aufgrund bestehender inhärenter Grenzen von Systemen können diese Maßnahmen die Kriterien nur mit hinreichender statt absoluter Sicherheit erfüllen.

Die Kriterien zur Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters sowie zur Geeignetheit der umzusetzenden Maßnahmen umfassen die in dem IDW Prüfungshinweis: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021) für das Cloud-Servicemodell „beesite Recruiting“ enthaltenen Ziele.

Verantwortung des Wirtschaftsprüfers

Unsere Aufgabe ist es, auf der Grundlage unserer Prüfung ein Urteil mit hinreichender Sicherheit darüber abzugeben, ob die Erklärung der gesetzlichen Vertreter von milch & zucker in allen wesentlichen Belangen frei von wesentlichen Fehlern ist. Dieses Urteil erstreckt sich auch darauf, ob die in der Erklärung der gesetzlichen Vertreter beschriebenen und von mich & zucker umzusetzenden Maßnahmen in allen wesentlichen Belangen

- geeignet waren und
- im geprüften Zeitraum (1. Juni bis 31. Dezember 2025) implementiert und wirksam waren.

Wir haben unsere Prüfung unter Beachtung des IDW Prüfungsstandards: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860) und des IDW Prüfungshinweises: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3 n.F.) (10.2021) durchgeführt.

Die in der Beschreibung der gesetzlichen Vertreter (Anlage 1) dargestellten Kriterien, die nicht Teil der Beschreibung waren, waren ebenso nicht Prüfungsgegenstand.

Unsere Wirtschaftsprüfungsgesellschaft hat die Anforderungen an das Qualitätssicherungssystem des IDW Qualitätssicherungsstandards: Anforderungen an das Qualitätsmanagement in der Wirtschaftsprüferpraxis (IDW QMS 1 (09.2022)) angewendet. Die Berufspflichten gemäß der WPO und der BS WP/vBP einschließlich der Anforderungen an die Unabhängigkeit haben wir eingehalten.

Nach diesen Anforderungen haben wir die Prüfung so zu planen und durchzuführen, dass wir mit hinreichender Sicherheit die vorgenannten Urteile abgeben können.

Eine Prüfung gemäß IDW PS 860 und IDW PH 9.860.3 n.F. (10.2021) umfasst die Durchführung von Prüfungshandlungen zur Erlangung ausreichender geeigneter Prüfungsnachweise, um entsprechende Prüfungsurteile abgeben zu können. Dies schließt die Beurteilung von Risiken wesentlicher - beabsichtigter oder unbeabsichtigter - Fehler in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters ein. Eine Prüfung umfasst auch die Beurteilung der bei der Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters angewandten Grundsätze, Verfahren und Maßnahmen sowie der Vertretbarkeit des von den gesetzlichen Vertretern ausgeübten Ermessens.

Ziel hierbei ist es jedoch nicht, ein Prüfungsurteil über das für die Aufstellung der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters relevante interne Kontrollsystem abzugeben.

Für die Beurteilung der umzusetzenden Maßnahmen ist die Prüfung so zu planen und durchzuführen, dass wesentliche Mängel der Geeignetheit und Implementierung der umgesetzten Maßnahmen mit hinreichender Sicherheit aufgedeckt werden. Diese Prüfung umfasst die Durchführung von Prüfungshandlungen im Rahmen einer Aufbauprüfung zur Erlangung ausreichender geeigneter Prüfungsnachweise, um ein entsprechendes Prüfungsurteil abgeben zu können.

Prüfungshandlungen und Prüfungsfeststellungen

Die Auswahl der Prüfungshandlungen liegt im pflichtgemäßen Ermessen des Wirtschaftsprüfers. Im Rahmen unseres Auftrags haben wir u.a. die folgenden Prüfungshandlungen überwiegend auf der Basis einer Auswahl durchgeführt:

- Befragung von Mitarbeitern
- Einsichtnahme in Unterlagen und Dokumentationen, wie bspw. Richtlinien, Arbeits- und Verfahrensanweisungen, Prozessdokumentationen
- Durchsicht von Nachweisen über die Umsetzung und Durchführung der Maßnahmen
- Systemeinsichtnahmen

Die Ergebnisse der von uns durchgeführten Prüfungshandlungen sowie die im Rahmen unserer Prüfung getroffenen Feststellungen sind in Anlage 2 aufgeführt.

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise ausreichend und geeignet sind, um als Grundlage für unser Prüfungsurteil zu dienen.

Prüfungsurteil

Nach unserer Beurteilung

- ist die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters in allen wesentlichen Belangen frei von wesentlichen Fehlern,
- war die in der Erklärung der gesetzlichen Vertreter des Cloud-Anbieters beschriebenen und vom Cloud-Anbieter umzusetzenden Maßnahmen in allen wesentlichen Belangen
    - geeignet und
    - im geprüften Zeitraum (1. Juni bis 31. Dezember 2025) implementiert sowie
    - im geprüften Zeitraum (1. Juni bis 31. Dezember 2025) wirksam

Inhärente Grenzen des geprüften für die Erbringung von Cloud-Diensten relevanten IT-Systems

Auch ein wirksames System unterliegt inhärenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird.

Die Erklärung der gesetzlichen Vertreter des Cloud-Anbieters zu den umzusetzenden Maßnahmen wurde zum 19. Dezember 2025 erstellt; die Ausführungen zu den Prüfungshandlungen zur Beurteilung der Geeignetheit und Implementierung dieser Maßnahmen erstrecken sich auf den Zeitraum vom 1. Juni bis 31. Dezember 2025. Eine Übertragung dieser Angaben auf einen zukünftigen Zeitpunkt birgt die Gefahr, dass aufgrund von durchgeführten Änderungen der Grundsätze, Verfahren und Maßnahmen falsche Schlussfolgerungen gezogen werden.

Verwendete Kriterien sowie Verwendungsbeschränkung

Ohne unser Urteil einzuschränken, verweisen wir auf die im Abschnitt „Verantwortung der gesetzlichen Vertreter“ beschriebenen Kriterien, die für Zwecke der Informationssicherheit des Cloud-Service konzipiert wurden. Die umzusetzenden Maßnahmen wurden durch milch & zucker abgegrenzt und beinhalten daher möglicherweise nicht jeden Aspekt, der aus individueller Sicht eines vorgesehenen Nutzers oder seines Abschlussprüfers ggf. von Bedeutung sein könnte.

Auftragsbedingungen

Wir erteilen diesen Prüfungsbericht auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten die diesem Prüfungsbericht beigefügten Allgemeinen Auftragsbedingungen (AAB) vom 1. Januar 2024 (Anlage 3) zugrunde liegen.

Bielefeld, 24. März 2026

HLB Dr. Stückmann und Partner mbB
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Gregor Teipel
Wirtschaftsprüfer

André Schneider
Certified Information Systems Auditor (CISA)

Anlagen

1. Erklärung der gesetzlichen Vertreter
2. Darstellung der geprüften Maßnahmen und der diesbezüglichen Prüfungshandlungen und Ergebnisse
3. Allgemeine Auftragsbedingungen