



**Kisters AG**

**Aachen**

**P R Ü F U N G S U R T E I L**

des für die Sicherheit, Vertraulichkeit und Verfügbarkeit relevanten Cloud-Services der Kisters AG mit Bericht des unabhängigen Wirtschaftsprüfers,  
einschließlich durchgeföhrter Tests und deren Ergebnisse

**für den Zeitraum  
vom 01.07.2024 bis 30.06.2025**

**System and Organization Controls (SOC) 2 Type 2 Report**  
unter Beachtung des  
**International Standard on Assurance Engagements (ISAE) 3000 (Revised)**

## Bericht eines unabhängigen Prüfers

Bericht des unabhängigen Wirtschaftsprüfers  
an den Vorstand der Kisters AG

### *Umfang*

Wir haben die in der Anlage 2 beigefügte Beschreibung mit der Überschrift "Anlage 2 – Systembeschreibung des Cloud – Dienstes" (Beschreibung) auf der Grundlage der Kriterien in Absatz 1.34 des AICPA-Leitfadens "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2<sup>SM</sup>)*" (Beschreibungskriterien) und die Eignung der Konzeption und der operativen Wirksamkeit der darin beschriebenen Kontrollen zur Erfüllung der Kriterien für die Sicherheits-, Vertraulichkeits- und Verfügbarkeitsgrundsätze, die in TSP-Abschnitt 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids)*, dargelegt sind (geltende trust services criteria), für den gesamten Zeitraum vom 01.07.2024 bis 30.06.2025 geprüft.

Die Informationen über die Zukunftspläne der Kisters AG für neue Systeme wurden nicht den Verfahren unterzogen, die bei der Prüfung der Beschreibung des Cloud-Service-Produkts und der Eignung der Konzeption und der operativen Wirksamkeit der Kontrollen angewendet wurden, um die entsprechenden geltenden trust services criteria zu erfüllen, die in der Beschreibung des Cloud-Service-Produkts angegeben sind.

### *Verantwortlichkeiten der Serviceorganisation*

Die Kisters AG hat ihre begleitende Erklärung mit dem Titel "Erklärung der gesetzlichen Vertreter (inkl. der Darstellung des Cloud-Dienstes und der vom Cloud-Anbieter angewendeten Grundsätze, Verfahren und Maßnahmen)" in Bezug auf die Angemessenheit der Darstellung der Beschreibung auf der Grundlage der Beschreibungskriterien und der Eignung der Konzeption und der operativen Wirksamkeit der darin beschriebenen Kontrollen zur Erfüllung der geltenden trust services criteria vorgelegt.

Die Kisters AG ist verantwortlich für (1) die Erstellung der Beschreibung und der Erklärung; (2) die Vollständigkeit, Richtigkeit und Art der Darstellung sowohl der Beschreibung als auch der Erklärung; (3) die Erbringung der von der Beschreibung abgedeckten Dienstleistungen; (4) die Festlegung der Kontrollen, die die geltenden trust services criteria erfüllen, und deren Angabe in der Beschreibung; und (5) die Konzeption, Implementierung und Dokumentation der Kontrollen zur Erfüllung der geltenden trust services criteria.

### *Verantwortlichkeiten des Prüfers*

Unsere Aufgabe ist es,

- ein Urteil über die Angemessenheit der Darstellung auf der Grundlage der Beschreibungskriterien abzugeben; und
- auf der Grundlage unserer Prüfung ein Urteil über die Eignung der Konzeption und der operativen Wirksamkeit der Kontrollen zur Erfüllung der geltenden trust services criteria abzugeben.

Wir haben unsere Prüfung in Übereinstimmung mit den vom American Institute of Certified Public Accountants festgelegten Prüfungsstandards durchgeführt. Danach ist unsere Prüfung so zu planen und durchzuführen, dass mit hinreichender Sicherheit festgestellt werden kann, ob (1) die Beschreibung auf der Grundlage der Beschreibungskriterien ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt und (2) die Kontrollen angemessen konzipiert waren und wirksam funktionierten, um die geltenden trust services criteria im gesamten Zeitraum vom 01.07.2024 bis 30.06.2025 zu erfüllen.

Wir haben überdies unsere Prüfung unter Beachtung des International Standard on Assurance Engagements (ISAE) 3000 (Revised) „Assurance Engagements Other Than Audits or Reviews of Historical Financial Information“ vorgenommen.

Unsere Prüfung umfasst die Durchführung von Verfahren zur Erlangung von Nachweisen über (1) die Angemessenheit der Darstellung der Erklärung auf der Grundlage der Erklärungskriterien und (2) die Eignung der Gestaltung und der operativen Wirksamkeit dieser Kontrollen zur Erfüllung der geltenden trust services criteria. Unsere Verfahren umfassen die Bewertung der Risiken, dass die Erklärung nicht den tatsächlichen Verhältnissen entspricht und dass die Kontrollen nicht angemessen konzipiert waren oder dass die Kontrollen nicht angemessen konzipiert sind oder nicht wirksam funktionieren, um die geltenden trust services criteria zu erfüllen.

Unsere Verfahren umfassten auch die Prüfung der operativen Wirksamkeit derjenigen Kontrollen, die wir für notwendig erachten, um mit hinreichender Sicherheit zu gewährleisten, dass die geltenden trust services criteria erfüllt wurden. Unsere Prüfung umfasste auch eine Bewertung der Gesamtdarstellung der Erklärung. Wir sind der Auffassung, dass die von uns erlangten Nachweise ausreichend und geeignet sind, um eine angemessene Grundlage für unser Urteil zu bilden.

### *Inhärente Grenzen*

Aufgrund ihres Charakters und ihrer inhärenten Grenzen funktionieren die Kontrollen in einer Dienstleistungsorganisation nicht immer effektiv, um die geltenden trust services criteria zu erfüllen. Auch die Projektion einer Bewertung der Angemessenheit der Darstellung der Beschreibung oder der Schlussfolgerungen über die Eignung der Konzeption oder der operativen Wirksamkeit der Kontrollen zur Erfüllung der geltenden trust services criteria in die Zukunft unterliegt dem Risiko, dass sich das System ändert oder dass die Kontrollen in einer Dienstleistungsorganisation unzureichend werden oder versagen.

### *Stellungnahme*

Nach unserer Auffassung

- a. vermittelt die Beschreibung auf der Grundlage der in der Erklärung von Kisters AG genannten Beschreibungskriterien und der geltenden trust services criteria in allen wesentlichen Belangen ein den tatsächlichen Verhältnissen entsprechendes Bild des Systems, das für den Zeitraum vom 01.07.2024 bis 30.06.2025 konzipiert und umgesetzt wurde;
- b. waren die in der Beschreibung genannten Kontrollen auf der Grundlage der in der Erklärung der Kisters AG genannten Beschreibungskriterien und der geltenden trust services criteria in allen wesentlichen Belangen so konzipiert, dass sie hinreichende Gewähr dafür bieten, dass die geltenden trust services criteria erfüllt würden, wenn die Kontrollen im gesamten Zeitraum vom 01.07.2024 bis 30.06.2025 wirksam funktioniert hätten;
- c. haben die getesteten Kontrollen auf der Grundlage, der in der Erklärung von Kisters AG genannten Beschreibungskriterien und der geltenden trust services criteria in allen wesentlichen Belangen wirksam funktioniert, d. h. sie waren, wenn sie wirksam waren, notwendig, um hinreichend sicherzustellen, dass die geltenden
- d. trust services criteria im gesamten Zeitraum vom 01.07.2024 bis 30.06.2025 erfüllt wurden.

### *Beschreibung der Kontrolltests*

Die spezifischen Kontrollen, die getestet wurden, sowie die Art, der Zeitpunkt und die Ergebnisse dieser Tests sind im Abschnitt „Geltende Trust Services Principles, Criteria, und damit zusammenhängende Kontrollen, Prüfungshandlungen und Ergebnisse der Prüfungshandlungen“ dieses Typ-2-Berichts in den Spalten 2, 4 bzw. 5 dargestellt.

### *Eingeschränkte Nutzung*

Dieser Bericht und die Beschreibung der Kontrolltests und deren Ergebnisse sind ausschließlich zur Information und zur Verwendung durch die Kisters AG , die Nutzer des Cloud-Service-Produkts der Kisters AG während des gesamten oder eines Teils des Zeitraums vom 01.07.2024 bis 30.06.2025 sowie durch potenzielle Nutzer, unabhängige Wirtschaftsprüfer und Fachleute, die Dienstleistungen für solche Nutzer erbringen, und Aufsichtsbehörden bestimmt, die über ausreichende Kenntnisse und Verständnis der folgenden Punkte verfügen:

- die Art der von der Dienstleistungsorganisation erbrachten Dienstleistung
- wie das System der Serviceorganisation mit den Benutzereinheiten oder anderen Parteien interagiert
- interne Kontrolle und ihre Grenzen
- die geltenden trust services criteria
- die Risiken, die die Erfüllung der geltenden trust services criteria gefährden können, und die Art und Weise, wie die Kontrollen diese Risiken angehen

### Auftragsbedingungen

Wir erteilen diesen Prüfungsvermerk auf Grundlage des mit der Gesellschaft geschlossenen Auftrags, dem auch mit Wirkung gegenüber Dritten gegenüber die diesem Prüfungsvermerk beigefügten Allgemeinen Auftragsbedingungen für Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften vom 01.01.2024 zugrunde liegen.

Köln, 24. November 2025

HKKG GmbH  
Wirtschaftsprüfungsgesellschaft



Diplom-Kaufmann (FH)  
Andreas Glasmacher  
Wirtschaftsprüfer



ppa.  
Lukas Ernst, M.A.  
Leiter IT- und ISMS-Prüfungen  
ISMS Auditor / Lead Auditor nach ISO 27001



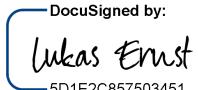
DocuSigned by:



Andreas Glasmacher

FB38471E06E6452...

DocuSigned by:



Lukas Ernst

5D1E2C857503451...

