KANTAR

Informations-Sicherheits-Management-System (ISMS)

Leitlinie

Kantar GmbH

KANTAR

Inhalt

KANTAR

Dokumentenlenkung

Eigentümer	Informationssicherheitsbeauftragte Kantar GmbH
Klassifizierung	Public (Green)
Gültigkeit	Ab 15.07.2012, unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	Q1/2027

Versionshistorie und Freigaben

Datum	Version	Autor	Veränderung	Freigabe durch	Status
09.07.2012	0.1	Dirk Wocke	Initiale Erstellung		draft
15.07.2012	1.0	Dirk Wocke	Kleinere Korrekturen	Oliver Bauchinger	freigegeben
23.07.2012	1.1	Dirk Wocke	Korrekturen & Unterschriftenblatt	Oliver Bauchinger	freigegeben
11.09.2012	2.0	Dirk Wocke	Korrekturen (in Absprache mit GBR) IT- Sicherheit durch Informationssicherheit ersetzt	Oliver Bauchinger	freigegeben
08.10.2013	2.0	Dirk Wocke	Review 2013 - keine Änderungen	Oliver Bauchinger	freigegeben
15.10.2014	2.0	Dirk Wocke	Review 2014 - keine Änderungen	Oliver Bauchinger	freigegeben
23.10.2015	2.0	Dirk Wocke	Review 2015 - keine Änderungen	Oliver Bauchinger	freigegeben
16.10.2016	2.0	Dirk Wocke	Review 2016 - keine Änderungen	Henk Hoogeveen	freigegeben
20.10.2017	2.1	Dirk Wocke	Review 2017 - KANTAR Logo eingefügt, TNS Infratest durch KANTAR ersetzt	Henk Hoogeveen	freigegeben
21.11.2018	2.1	Dirk Wocke	Review 2018 - keine Änderungen	Henk Hoogeveen	freigegeben
06.11.2019	2.2	Dirk Wocke	Review 2019 - KANTAR Deutschland durch KANTAR ersetzt	Henk Hoogeveen	freigegeben
12.11.2020	2.2	Dirk Wocke	Review 2020 – keine Änderungen	Henk Hoogeveen	freigegeben

KANTAR

Datum	Version	Autor	Veränderung	Freigabe durch	Status
18.11.2021	2.4	Dirk Wocke	Review 2021 - keine Änderungen	Henk Hoogeveen	freigegeben
18.11.2022	2.3	Dirk Wocke	Review 2022 - Kleinere Korrekturen	Andreas Pohle	freigegeben
17.11.2023	2.5	Dirk Wocke	Review 2023 - Kleinere Korrekturen	Andreas Pohle	freigegeben
18.02.2025	3.0	Isabelle Zieglmaier	Vollständige Überarbeitung	Andreas Pohle	freigegeben
16.02.2026	3.1	Isabelle Zieglmaier	Review 2026 - Aufnahme strategische KI-Ausrichtung	Andreas Pohle	freigegeben

KANTAR

1. Einleitung

1.1. Motivation

Die Kantar GmbH muss unter Beachtung der rechtlichen und wirtschaftlichen Rahmenbedingungen sowie den Anforderungen aus ihren **Geschäftsprozessen** wirtschaftlich, effizient, nachvollziehbar und dienstleistungsorientiert handeln. Der Einsatz von Informationstechnologie optimiert die Geschäftsprozesse zur Leistungssteigerung, eröffnet jedoch – etwa durch neue Technologien wie Künstliche Intelligenz (KI) – neue Gefährdungsquellen. Daher müssen Geschäftsprozesse im Rahmen des **Risikomanagements** sicher gestaltet und betrieben werden.

Jede Beeinträchtigung der **Informationssicherheit** kann die Leistungsfähigkeit der Kantar GmbH mindern oder Geschäftsprozesse zum Erliegen bringen, was erheblichen Schaden verursachen kann. Zur langfristigen Sicherung der Informationssicherheit und Schadensabwehr sind die Initiierung und Etablierung eines ganzheitlichen **Informationssicherheitsprozesses** erforderlich.

Informationssicherheit ist ein vitales Interesse der Kantar GmbH und somit ein wichtiges strategisches Ziel.

1.2. Ziele

Diese Leitlinie ist das **strategische Basis-Dokument zur Sicherstellung der Informationssicherheit** für durch Informationstechnologie unterstützte Geschäftsprozesse. Sie ist Grundlage für alle Maßnahmen und Handlungen innerhalb der Geschäftsprozesse

Informationssicherheit ist integraler und essenzieller Bestandteil jedes Handelns und muss daher immer berücksichtigt werden. Sie dient der Wahrung der nachfolgenden Grundeigenschaften von Informationen:

- **Vertraulichkeit**
  Informationen oder Funktionen (Hardware, Software, Arbeitsprozess) dürfen nur dem berechtigten Personenkreis zur Verfügung stehen.

- **Integrität**
  Die Unversehrtheit von Informationen ist jederzeit sicherzustellen. Informationen müssen korrekt und vollständig sein, Funktionen müssen korrekte Ergebnisse liefern.

- **Verfügbarkeit**
  Die Nutzung von Informationen oder Funktionen muss dem berechtigten Personenkreis in dem benötigten Zeitraum mit der erforderlichen Güte möglich sein.

KANTAR

Ziel ist es, das jeweils erforderliche Informationssicherheitsniveau zum Schutz aller Geschäftsprozesse und deren Informationen durch angemessene und zielführende organisatorische und technische Maßnahmen sicherzustellen.

Der **Datenschutz** schützt das Grundrecht auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten. Dafür müssen die Grundeigenschaften dieser Informationen gewahrt werden. Die Datenschutzvorgaben stellen besondere Anforderungen an die Informationssicherheit.

2. Geltungsbereich

Diese Richtlinie gilt für alle Bereiche der Kantar GmbH, in denen Informationen verarbeitet werden. Die Vorgaben sind in allen Geschäftsprozessen während ihres gesamten Lebenszyklus zu befolgen.

Sie ist für alle Mitarbeitenden der Kantar GmbH verbindlich.

Wird Dritten außerhalb der Kantar GmbH Zugang zu Informationen oder IT gewährt, müssen sie durch entsprechende Vereinbarungen zur Einhaltung dieser Richtlinie verpflichtet werden. Die Einhaltung ist nachzuweisen und kann vom zuständigen Informationssicherheitsbeauftragten überprüft werden.

3. Prinzipien

Um die Informationen in den Geschäftsprozessen gemäß den Zielen der Informationssicherheit effizient und zielführend schützen zu können, ergänzen folgende Prinzipien die Informationssicherheitsstrategie der Kantar GmbH:

- **Prävention:** Das Risiko bei der Verarbeitung von Informationen in Geschäftsprozessen ist durch vorbeugende Maßnahmen zu minimieren. Alle Beschäftigten sind regelmäßig zu sensibilisieren.

- **Reaktion:** Bei Gefährdungen ist durch geplantes Vorgehen zu reagieren. Rechtzeitige Erkennung und vorbereitete Reaktionen sollen negative Beeinträchtigungen minimieren.

- **Nachhaltigkeit:** Maßnahmen müssen gewährleisten, dass das Informationssicherheitsniveau während des gesamten Lebenszyklus eines Prozesses aufrechterhalten wird. Das Sicherheitsniveau wird regelmäßig überprüft und Maßnahmen ergriffen, um die notwendige Sicherheit weiterhin zu gewährleisten.

Aus den **strategischen Zielen der Kantar GmbH** und dieser Leitlinie ergeben sich hinsichtlich der Informationssicherheit organisatorische und technische Anforderungen an unsere Geschäftsprozesse. Diese sind effizient, wirtschaftlich und zielführend umzusetzen. Angemessene Investitionen in Informationssicherheit sind notwendig.

Schulungs- und Sensibilisierungsmaßnahmen sind für die Erreichung der Ziele der Informationssicherheit unabdingbar. Die Teilnahme an diesen Maßnahmen ist für alle Mitarbeitenden verpflichtend.

4. Rahmenbedingungen

Die Kantar GmbH muss eine **Vielzahl von gesetzlichen Vorgaben und Standards** einhalten, um die Informationssicherheit zu gewährleisten. Dazu gehören u.a. die Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG), das IT-Sicherheitsgesetz sowie die EU-Verordnung zur Künstlichen Intelligenz (EU AI Act). Diese gesetzlichen Rahmenbedingungen legen z.B. fest, wie personenbezogene Daten zu schützen, welche technischen und organisatorischen Maßnahmen zu ergreifen und wie Sicherheitsvorfälle zu melden sind.

Die Einhaltung dieser Vorgaben ist unerlässlich, um rechtliche Konsequenzen zu vermeiden und das Vertrauen der Kunden und Partner zu sichern. Darüber hinaus müssen alle Datenschutzvorgaben und speziellen Sicherheitsstandards, die auf **Konzernebene** festgelegt werden, von der Kantar GmbH beachtet werden. Zudem wird die gesamte IT-Infrastruktur von Kantar Global bereitgestellt.

Im Rahmen der konzernweiten Digitalisierungsstrategie setzt Kantar verstärkt auf den Einsatz von Künstlicher Intelligenz (KI), insbesondere durch die Integration von Microsoft M365 Copilot in die täglichen Arbeitsprozesse. Die Kantar GmbH folgt dieser strategischen Ausrichtung und nutzt KI-Technologien gezielt zur Prozessoptimierung, Leistungs- und Qualitätssteigerung. Dabei wird sichergestellt, dass alle eingesetzten KI-Systeme den geltenden rechtlichen Anforderungen entsprechen. Insbesondere werden keine Hochrisiko-Anwendungen im Sinne des EU AI Act betrieben. Die Nutzung von KI erfolgt unter strikter Einhaltung der Datenschutzvorgaben, internen Richtlinien sowie einer Gesamtbetriebsvereinbarung zu M365 Copilot. Die Mitarbeitenden sind angehalten, KI verantwortungsvoll und mit der gebotenen Sorgfalt in ihre Arbeitsabläufe zu integrieren.

KANTAR

5. Informationssicherheitsprozess

Der Informationssicherheitsprozess der Kantar GmbH gewährleistet durch geplantes und organisiertes Vorgehen die Erreichung der Sicherheitsziele. Die Initiierung umfasst die Erstellung und verbindliche Einführung der Leitlinie und der Organisationsstruktur für die Informationssicherheit.

Um die Angemessenheit und Wirksamkeit des Sicherheitsmanagements sicherzustellen, wird der gesamte Prozess kontinuierlich einem PDCA-Zyklus unterzogen:

- **Erstellung von Sicherheitsrichtlinien und -konzepten:** Diese bilden die Grundlage für alle nachfolgenden Prozessphasen
- **Analyse des Ist-Zustandes:** Feststellung des aktuellen Zustands zur Informations-sicherheit und Festlegung des Soll-Zustands
- **Etablierung und Umsetzung:** Planung und Umsetzung der erforderlichen Maßnahmen zur Erreichung des definierten Sicherheitsniveaus
- **Informationssicherheit im laufenden Geschäftsprozess:** Fortlaufende Überwachung der Einhaltung gesetzlicher und interner Vorgaben
- **Revision:** Vergleich des aktuellen Zustands mit den dokumentierten Vorgaben und Optimierung der Maßnahmen
- **Audit:** Regelmäßige Überprüfung der Umsetzung und Wirksamkeit der Maßnahmen

Dieser Prozess stellt sicher, dass die Informationssicherheit stets gewährleistet und den aktuellen Erfordernissen angepasst wird.

6. Rollen und Verantwortlichkeiten

Fehlende oder unklare Verantwortlichkeiten gefährden die sichere Abwicklung von Geschäftsprozessen und des IT-Betriebs. Daher ist es unerlässlich, Rollen und Verantwortlichkeiten der Informationssicherheitsprozesse der Kantar GmbH klar zu definieren.

- Die **oberste Leitungsebene** ist verantwortlich für die Informationssicherheit und muss sicherstellen, dass diese Leitlinie zielführend und effizient umgesetzt wird. Sie überwacht die Wirksamkeit von Maßnahmen und veranlasst bei Bedarf Verbesserungen.
- **Führungskräfte** müssen sicherstellen, dass ihre Mitarbeitenden sicherheitskonform handeln und das Sicherheitsbewusstsein fördern.

- **Prozesseigentümer** tragen die Gesamtverantwortung für ihre Prozesse und müssen sicherstellen, dass Informationen angemessen geschützt sind.

- **Projektverantwortliche** sind für die Sicherheitsbelange von der Projektbeauftragung bis zum Projektergebnis verantwortlich.

- Alle Mitarbeitenden übernehmen die Rolle der **Informationsverantwortlichen** ("Informationseigentümer") und sind für die Klassifizierung der Informationen zuständig. Der Schutzbedarf dieser Informationen variiert je nach Prozess, vertraglicher Vereinbarungen und gesetzlicher Vorgaben. Informationsverantwortliche bestimmen den erforderlichen Schutzbedarf und leiten daraus organisatorische sowie technische Maßnahmen ab, um den entsprechenden Schutz sicherzustellen.

Informationssicherheitsbeauftragte sind für die Fortschreibung und die Koordination des Informationssicherheitsmanagementsystems (ISMS) verantwortlich. Sie überprüfen regelmäßig die Einhaltung der Vorgaben für die Informationssicherheit. Zu den Hauptaufgaben gehören die Identifizierung und Bewertung von Sicherheitsrisiken sowie die regelmäßige Überprüfung der Einhaltung der Vorgaben für die Informationssicherheit.

Datenschutzbeauftragte sind eigenständig. Ihre Aufgabe innerhalb des Informationssicherheitsprozesses ist es, sicherzustellen, dass die gesetzlichen Auflagen bezüglich des Grundrechtes auf informationelle Selbstbestimmung (Datenschutz) eingehalten werden.

AI-Beauftragte sind verantwortlich für die Steuerung und Kontrolle des KI-Einsatzes innerhalb Kantars. Zu den Aufgaben gehören die Entwicklung und Pflege von Richtlinien für den sicheren und gesetzeskonformen Einsatz von KI-Systemen, insbesondere im Einklang mit der EU-Verordnung zur Künstlichen Intelligenz (EU AI Act), der Datenschutz-Grundverordnung (DSGVO) sowie der Betriebsvereinbarung zu M365 Copilot. Die AI-Beauftragten arbeiten eng mit der Informationssicherheits- und Datenschutzorganisation zusammen, bewerten KI-bezogene Risiken und stellen sicher, dass Mitarbeitende über die geltenden Vorgaben informiert und entsprechend geschult sind.

Die **Informationssicherheitsorganisation** umfasst zudem Bereichs- und Standortbeauftragte. Diese Organisation trifft sich regelmäßig, um sich über Themen der Informationssicherheit und des Datenschutzes auszutauschen. Zu ihren Hauptaufgaben zählen die Überprüfung der effektiven Umsetzung von Sicherheitsmaßnahmen sowie bei Bedarf die Sensibilisierung der betreuten Mitarbeitenden.

Die **IT-Verantwortlichen** fungieren als zentrale Instanz für die operative IT-Sicherheit und sind zuständig für den sicheren Betrieb der IT sowie die Implementierung geeigneter Sicherheitsmechanismen. Durch die systematische Identifizierung und Minderung von Schwachstellen tragen sie zur Erhöhung der Informationssicherheit bei und demonstrieren gegenüber Kunden und Partnern das Engagement des Unternehmens für den Schutz sensibler Daten. Die IT-

Verantwortlichen gewährleistet zudem, dass die Informationssicherheitsbeauftragten frühzeitig in die relevanten IT-Projekte eingebunden werden.

Alle Beschäftigten der Kantar GmbH haben jederzeit – den Umständen entsprechend – ihr Möglichstes zu unternehmen, um die Informationssicherheit in ihrem Aufgabenbereich aufrechtzuerhalten. Sie müssen sicherstellen, dass sie alle Sicherheitsmaßnahmen verstehen und befolgen, die vorgeschrieben sind, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme der Organisation zu gewährleisten. Insbesondere haben sie die zuständigen Informationssicherheitsbeauftragten bei der Erledigung ihrer Aufgaben aktiv zu unterstützen (Informationspflicht). Mitarbeitende sollten aufmerksam sein und verdächtige Aktivitäten oder ungewöhnliches Verhalten an die Informationssicherheitsorganisation melden.
Darüber hinaus sind alle Mitarbeitenden angehalten, neue Technologien wie Künstliche Intelligenz (KI) verantwortungsvoll in ihre Arbeitsprozesse zu integrieren. Die Nutzung von KI-gestützten Tools – wie z. B. M365 Copilot – ist ausdrücklich erwünscht, sofern die geltenden Vorgaben (z. B. Datenschutz, kein Missbrauch, keine Diskriminierung) eingehalten werden. KI-generierte Inhalte sind stets mit der gebotenen Sorgfalt zu prüfen, bevor sie weiterverwendet oder weitergegeben werden. Die Einhaltung der in der Gesamtbetriebsvereinbarung definierten Regeln ist verpflichtend.

7. Dokumentation

Die Informationssicherheitsdokumente der Kantar GmbH orientieren sich an den Vorschlägen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Alle Dokumente werden sach- und zielgruppenorientiert erstellt und bedarfsgerecht fortgeschrieben. Dies sorgt für eine einheitliche Bewertung, Nachvollziehbarkeit und Vergleichbarkeit von Sicherheitsmaßnahmen bei Audits und Revisionen.

8. Sensibilisierung zu Risiken der IT-Nutzung

Für Mitarbeitende sind regelmäßige Informations- und Sensibilisierungsmaßnahmen sowie Schulungen zu Themen der Informationssicherheit durchzuführen. Verhaltensregeln sind schriftlich zu dokumentieren und auf geeignete Weise bereitzustellen.

Mitarbeitende im IT-Umfeld müssen regelmäßig über sicherheitsrelevante Entwicklungen informiert werden und sich fach- und aufgabenspezifisch weiterbilden. Dies gilt insbesondere für Beschäftigte, die in die Organisationsstruktur für Informationssicherheit eingebunden sind.

Ergänzend hierzu werden umfassende Schulungsmaßnahmen zum sicheren und effektiven Einsatz von Künstlicher Intelligenz (KI) angeboten. Dazu zählen unter anderem verpflichtende Basisschulungen, praxisorientierte Webinare sowie eLearning-Programme. Ziel dieser Maßnahmen ist es, die Mitarbeitenden zu befähigen, KI-Tools wie M365 Copilot sicher, effizient und im Einklang mit den geltenden Richtlinien zu nutzen.

9. Verstöße gegen die Informationssicherheit

9.1. Meldung von Auffälligkeiten oder Verstößen

Alle Mitarbeitenden sind unabhängig von der Funktion berechtigt und aufgefordert, Auffälligkeiten oder mögliche Verstöße gegen die Informationssicherheit unverzüglich zu melden.

9.2. Konsequenzen bei Verstößen

Verstöße gegen Sicherheitsvorgaben können der Organisation, den Mitarbeitenden, Geschäftspartnern und Kunden Schaden zufügen.

Unbeabsichtigte Verstöße können auch bei sorgfältiger Arbeit vorkommen und bleiben in der Regel ohne Folgen für die Betroffenen, wenn sie unverzüglich gemeldet werden.
Vorsätzliche Verstöße gegen Sicherheitsvorgaben können arbeits- oder strafrechtliche Konsequenzen nach sich ziehen.