KANTAR

# Datenschutzkonzept

## Organisation und Umsetzung des Datenschutzes

14.07.2022

Kantar GmbH
Infratest dimap Gesellschaft für Trend- und Wahlforschung mbH
Kantar Holding GmbH

(zusammen im Folgenden: “KANTAR”)

# Inhaltsverzeichnis

# Einleitung und Ziel des Datenschutzkonzepts

Das Thema Datenschutz ist für KANTAR von großer Wichtigkeit.

Während des Tagesgeschäfts werden in großem Umfang datenschutzrelevante Tätigkeiten durchgeführt. Dies betrifft sowohl personenbezogene Daten, die KANTAR selbst im Rahmen der Markt- und Sozialforschung erhebt oder von Kunden und Lieferanten zu diesem Zweck zur Verfügung gestellt bekommt, als auch selbstverständlich die personenbezogenen Daten eigener Beschäftigter und der Beschäftigten von bestehenden und potentiellen Geschäftspartnern.

Die Anforderungen an den Datenschutz und die Datensicherheit haben sich zum 25. Mai 2018 durch die ab dann verbindlich geltende EU-Datenschutzgrundverordnung (DSGVO) deutlich erhöht. Die DSGVO hat dabei die verschiedenen, bislang in Europa geltenden nationalen Datenschutzgesetze in weiten Teilen abgelöst und ein einheitliches Datenschutzrecht im Europäischen Wirtschaftsraum (EWR) geschaffen.

Den nationalen Gesetzgebern wurden in der DSGVO an einigen Stellen Regelungsspielräume eingeräumt. Von diesen hat der deutsche Gesetzgeber auch teilweise Gebrauch gemacht und dort ergänzende Regelungen (insbesondere in Bezug auf den Beschäftigtendatenschutz) getroffen. Neben der DSGVO wird daher in Einzelfällen immer noch das Bundesdatenschutzgesetz, nunmehr allerdings das neue Bundesdatenschutzgesetz (BDSG-neu) heranzuziehen sein, welches das bisherige Bundesdatenschutzgesetz (BDSG-alt) abgelöst hat.

Mit Einführung der DSGVO hat auch das gesellschaftliche und mediale Interesse an dem Thema Datenschutz zugenommen. Richtigerweise hat der Gesetzgeber die Rechte und Freiheiten der Betroffenen im Hinblick auf den Schutz ihrer Daten und ihr Recht auf informationelle Selbstbestimmung deutlich gestärkt.

Die Kerntätigkeit im Rahmen der Markt- und Sozialforschung ist es, Meinungen, Gedanken, Gefühle sowie das Verhalten von Menschen zu ermitteln. Insofern hat KANTAR eine besondere Verantwortung: Das Unternehmen muss jeden Tag aufs Neue im Umgang mit Daten beweisen, dass es das Vertrauen der Menschen, die sich ihm mitteilen, wert ist.

# 1. Allgemeine Angaben

### 1.1 Ziel des Datenschutzkonzepts

Das vorliegende Datenschutzkonzept enthält eine Beschreibung der Organisation und Umsetzung der datenschutzrechtlichen Verpflichtungen und bestimmt Aufgaben, Verpflichtungen und Verantwortlichkeiten sowie die Konditionen der Datenverarbeitungsprozesse im Unternehmen.

### 1.2 Verantwortliche Stellen

- **Kantar GmbH**, Landsberger Str. 284, 80687 München;

  eingetragen im Handelsregister des Amtsgerichts München unter HRB 114447.

- **Infratest dimap Gesellschaft für Trend- und Wahlforschung mbH**, Alt-Moabit 96a, 10559 Berlin;

  eingetragen im Handelsregister des Amtsgerichts Berlin unter HRB 35138.

- **Kantar Holding GmbH,** Landsberger Str. 284, 80687 München, Germany;

  eingetragen im Handelsregister des Amtsgerichts München unter HRB 114447.

### 1.3 Datenschutzbeauftragte

Martha Ferrari, LL.M.

Kantar GmbH, Landsberger Straße 284, 80687 München

E-Mail: datenschutz@kantar.com

### 1.4 Angaben zum Rechenzentrum

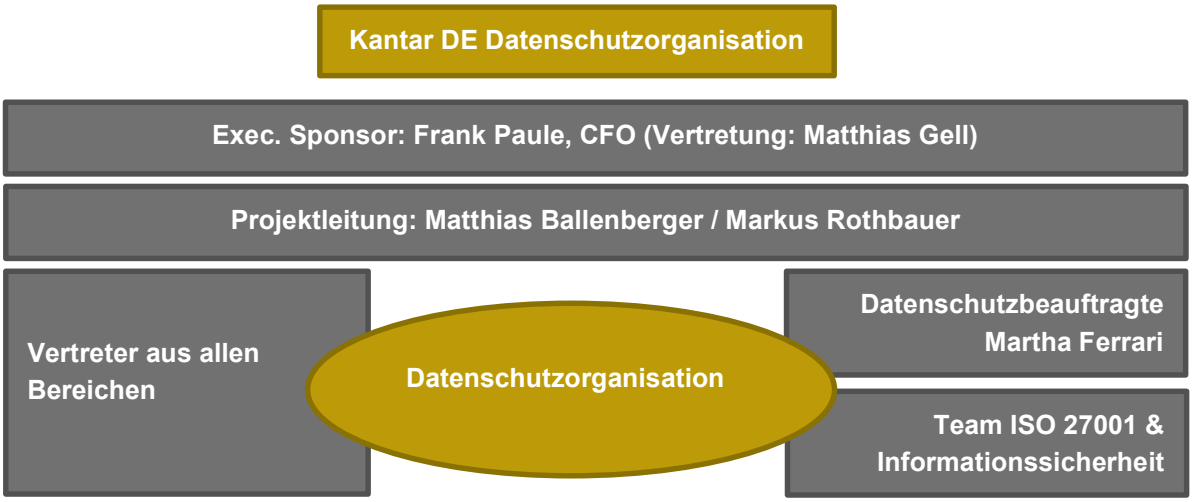
- Hochverfügbares IT-Rechenzentrum
- Alle IT-Prozesse sind ISO 20000-konform
- Umfangreiche SOX Controls

# 2. Organisation des Datenschutzes im Unternehmen

## 2.1 Beschreibung der Datenschutzorganisation

- KANTAR hat eine Datenschutzbeauftragte bestellt (vgl. Ziffer 1.3). Die Datenschutzbeauftragte berichtet direkt an die Geschäftsführung und ist Teil der Abteilung Datenschutz & Legal (bestehend aus vier Mitarbeitern).

- Zur kontinuierlichen Verbesserung der datenschutzrechtlich relevanten Prozesse existiert eine lokale Datenschutzorganisation.




- Ergänzend und auf globaler Ebene existiert das Kantar GDPR Programme. Die globale Organisation ist aufgeteilt in:

| |
|---|
| **Kantar GDPR Steering Board**<br>■ Strategische Vorgaben und Beratung des Kantar GDPR Programme<br>■ Lösung von Problemen außerhalb der Befugnisse des Kantar GDPR Programme<br>■ Bereitstellung von Ressourcen und Budget |
| **Privacy Office**<br>■ Treiber und Unterstützer des Kantar GDPR Programmes |

| |
|---|
| ■ Projektmanagement<br>■ Bereitstellung von Templates und Best Practice |
| **Accountability Leads (ALs)**<br>■ als Repräsentanten der verschiedenen OpBrands sowie von Finance und HR<br>■ Erstellung OpBrand-spezifischer Implementierungspläne |
| **Topic Advisory Groups (TAG)**<br>■ Formulierung der GDPR Policies für die OpBrands<br>■ Sicherstellung der Anwendbarkeit und Akzeptanz der Policies in den Kantar-Einheiten |

### 2.2 Datenschutzleitlinie und KANTARs zwölf Prinzipien im Datenschutz

KANTAR hat sich eine unternehmensinterne Datenschutzleitlinie auferlegt. Darin werden Erläuterungen und detaillierte Vorgaben zu den folgenden zwölf Prinzipien getroffen:

***1 – Privacy by Design***

Ich achte bei neuen Tools und Prozessen auf Datenschutzkonformität.

Bei der Entwicklung neuer Methoden, Software, Projektdesigns etc. ist das Datenschutzteam von Beginn an einzubinden.

***2 – Rechtmäßigkeit***

Ich erhebe / verarbeite Daten nur, wenn es gesetzlich erlaubt ist.

Im Grundsatz ist im Datenschutzrecht alles verboten, was nicht ausdrücklich erlaubt ist (Verbot mit Erlaubnisvorbehalt).

***3 – Zweckbindung***

Ich erhebe / verarbeite Daten nur für den ursprünglichen Zweck.

Vor Datenerhebung ist eindeutig und abschließend ein legitimer Zweck festzulegen und an die Betroffenen zu kommunizieren.

***4 – Datensicherheit***

Ich schütze die Daten angemessen.

Personenbezogene Daten sind angemessen vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung zu schützen.

***5 – Datenminimierung***

Ich erhebe / verarbeite nur die erforderlichen Daten.

Erhoben und verarbeitet werden nur die Daten, die zur Erfüllung des Zwecks in angemessenem Maß benötigt werden.

***6 – Pseudonymisierung***

Ich pseudonymisiere Daten so früh wie möglich.

Die Daten werden so getrennt, dass diese nur mit Hilfe einer separaten ID einer Person zuordenbar sind.

***7 – Speicherbegrenzung***

Ich behalte Daten nur solange ich sie benötige oder Gesetze es verlangen.

Im Grundsatz sollen personenbezogene Daten nur so lange wie nötig und so kurz wie möglich gespeichert werden.

***8 – Richtigkeit und Korrekturrecht***

Ich stelle sicher, dass die Daten sachlich richtig & aktuell sind.

Es werden angemessene Maßnahmen getroffen, um Datenbestände auf einem richtigen und aktuellen Stand zu halten.

***9 – Informationsrecht***

Ich informiere Betroffene über die Verwendung ihrer Daten.

Betroffene werden vor bzw. bei der Erhebung oder Verarbeitung ihrer Daten über deren Verwendung und ihre Rechte transparent informiert.

***10 – Auskunftsrecht***

Ich leite Auskunftsanfragen unverzüglich an den Datenschutz weiter.

Der Betroffene hat das Recht, zeitnah über seine gespeicherten Daten Auskunft zu erhalten.

***11 – Recht auf Vergessenwerden***

Ich leite Löschanfragen unverzüglich an den Datenschutz weiter.

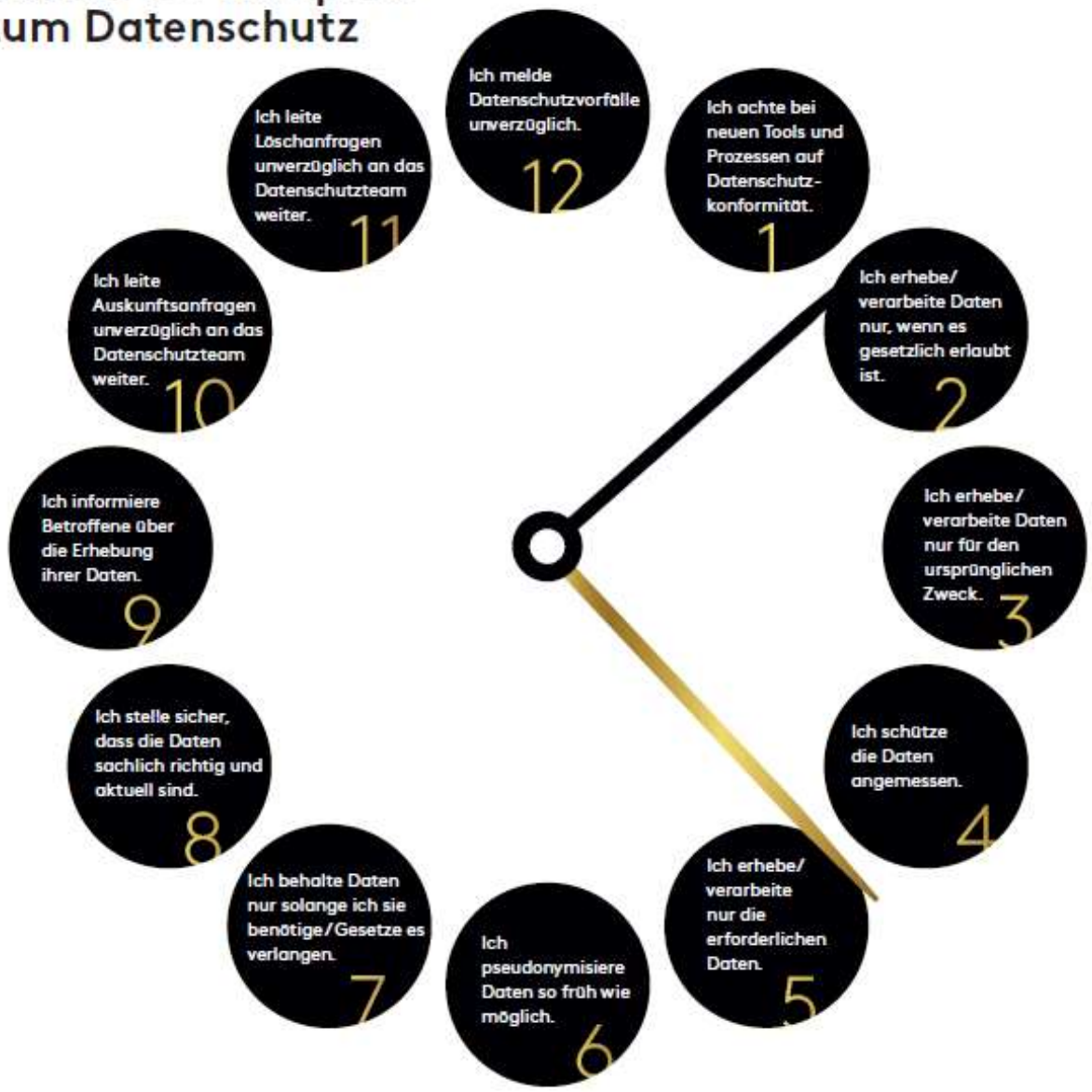
Der Betroffene hat das Recht auf eine zeitnahe Löschung seiner gespeicherten Daten (sofern gesetzlich zulässig).

***12 – Meldung von Datenschutzvorfällen***

Ich melde Datenschutzvorfälle unverzüglich.

Datenschutzvorfälle müssen unverzüglich, wie im Intranet beschrieben, gemeldet werden.

# Unsere 12 Prinzipien zum Datenschutz




1
Privacy by Design
Bei der Entwicklung von neuen Methoden, Software, Projektdesigns etc. ist das Datenschutzteam von Beginn an einzubinden.

2
Rechtmäßigkeit
Im Grundsatz ist im Datenschutzrecht alles verboten, was nicht ausdrücklich erlaubt ist (Verbot mit Erlaubnisvorbehalt).

3
Zweckbindung
Vor Datenerhebung ist eindeutig und abschließend ein legitimer Zweck festzulegen und an die Betroffenen zu kommunizieren.

4
Datensicherheit
Daten sind angemessen vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung zu schützen.

5
Datenminimierung
Erhoben und verarbeitet werden nur die Daten, die zur Erfüllung des Zwecks unbedingt benötigt werden.

6
Pseudonymisierung
Die Daten werden so getrennt, dass diese nur mit Hilfe einer separaten ID einer Person zuordenbar sind.

7
Speicherbegrenzung
Im Grundsatz sollen personenbezogene Daten nur so lange wie nötig und so kurz wie möglich gespeichert werden.

8
Richtigkeit und Korrekturrecht
Es werden angemessene Maßnahmen getroffen, um Datenbestände auf einem richtigen und aktuellen Stand zu halten.

9
Informationsrecht
Betroffene werden vor bzw. bei der Erhebung oder Verarbeitung ihrer Daten über deren Verwendung und ihre Rechte transparent informiert.

10
Auskunftsrecht
Der Betroffene hat das Recht, zeitnah über seine gespeicherten Daten Auskunft zu erhalten.

11
Recht auf Vergessenwerden
Der Betroffene hat das Recht auf eine zeitnahe Löschung seiner gespeicherten Daten (sofern gesetzlich zulässig).

12
Melden von Datenschutzvorfällen
Datenschutzvorfälle müssen unverzüglich, wie im Intranet beschrieben, gemeldet werden.

Weitere Informationen findest Du auf der Datenschutzseite im Intranet oder bei Deinem Datenschutzbeauftragten. Euer DSGVO-Team.

KANTAR

### 2.3 Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter

Sämtliche Mitarbeiter sind sowohl auf Vertraulichkeit und Datenschutz als auch auf das Sozialgeheimnis nach § 35 SGB I verpflichtet.

Sämtliche Mitarbeiter müssen einmal jährlich die Online-Schulungsmodule *Datenschutz* und *Informationssicherheit* erfolgreich absolvieren. Neue Mitarbeiter müssen direkt bei Eintritt die Online-Module absolvieren.

Jeder neue Mitarbeiter ist zudem verpflichtet, an der Schulung *Datenschutz und Informationssicherheit für Einsteiger* teilzunehmen, welche von der Datenschutzbeauftragten regelmäßig durchgeführt wird. Daneben können Mitarbeiter freiwillig an der Schulung *Datenschutz und Informationssicherheit für Fortgeschrittene* teilnehmen, welche ebenfalls von der Datenschutzbeauftragten regelmäßig durchgeführt wird.

# 3. Rechtliche Rahmenbedingungen und Einzelheiten der Verarbeitung

### 3.1 Zweckbestimmung und Rechtsgrundlagen für die Verarbeitung

Die Kantar GmbH erhebt, verarbeitet und nutzt personenbezogene Daten zu Zwecken der Markt- und Sozialforschung in nahezu allen gesellschaftlichen Bereichen (z. B. Technology & Finance, Media & Internet, Consumer & Industry, Mobility, Political & Social, etc.).

KANTAR erkennt den im Datenschutzrecht geltenden Grundsatz des Verbots mit Erlaubnisvorbehalt an und verarbeitet Daten daher stets nur bei Vorliegen der gesetzlich definierten Rechtsgrundlagen:

- Bei der Verarbeitung personenbezogener Daten für Zwecke der Markt- und Sozialforschung stützt sich KANTAR auf die verfügbaren Rechtsgrundlagen, insbesondere auf berechtigte Interessen gemäß Art. 6 Abs. 1 lit. f) DSGVO (Privilegierung der Markt- und Sozialforschung vormals in: § 30a BDSG-alt), bei wissenschaftlichen Forschungs- und Statistikvorhaben auf § 27 BDSG sowie die Einwilligung der Studienteilnehmer nach Art. 6 Abs. 1 lit. a) DSGVO.

  Sofern KANTAR personenbezogene Daten (z.B. Adressen) von Kunden erhält, ist für die Übermittlung an und weisungsgebundene Verarbeitung der Adressen durch KANTAR ein Vertrag über die Auftragsverarbeitung gemäß Art. 28 DSGVO zwischen dem Kunden als Verantwortlichen und KANTAR erforderlich.

  Besonders relevant für KANTAR im Rahmen der Sozialforschung und bei der Tätigkeit für öffentliche Auftraggeber sind daneben die Rechtsgrundlagen des § 46 Bundesmeldegesetz (BMG) zur Einholung einer Gruppenauskunft und des § 75 des Zehnten Buchs Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X) zum Erhalt von Sozialdaten für Zwecke der Arbeitsmarkt- und Berufsforschung.

- Bei der Verarbeitung personenbezogener Daten von KANTARs Beschäftigten stützt sich KANTAR auf die verfügbaren Rechtsgrundlagen, insbesondere auf Art. 6 Abs. 1 lit. b), c) und f) DSGVO sowie die Rechtsgrundlage des § 26 BDSG (neu) zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses.

- Bei der Verarbeitung personenbezogener Daten von Beschäftigten von KANTARs Kunden und Lieferanten stützt sich KANTAR auf die verfügbaren Rechtsgrundlagen, insbesondere auf Art. 6 Abs. 1 lit. b) und f) DSGVO.

### 3.2 Weitere Gesetze und ADM-Standesregeln

- Studien der Markt- und Sozialforschung: KANTAR ist Mitglied im Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM).

  Der ADM hat mit der Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V. (ASI), der Deutschen Gesellschaft für Online-Forschung e.V. (DGOF) sowie dem Berufsverband Deutscher Markt- und Sozialforscher e.V. (BVM) Richtlinien herausgegeben, die bei Studien der Markt- und Sozialforschung

verbindlich sind und in denen festgelegt ist, wie die Anforderungen des Datenschutzes in die Praxis der Markt- und Sozialforschung umzusetzen sind.

Zu den Standesregeln gehören ferner der „Internationale Kodex für die Praxis der Markt- und Sozialforschung“ von IHK/ESOMAR, kurz ESOMAR-Kodex, sowie die von ESOMAR für verschiedene Arbeitsgebiete der Markt- und Sozialforschung ebenfalls herausgegebenen ESOMAR-Richtlinien. Die oben genannten deutschen Instituts- und Berufsverbände haben zudem eine „Erklärung für das Gebiet der Bundesrepublik Deutschland zum IHK/ESOMAR Internationalen Kodex für die Praxis der Markt- und Sozialforschung“ her-ausgegeben, in der einige Regelungen des ESOMAR-Kodex modifiziert sind.

- Individualisierte Befragungen: Einzelne Befragungen von KANTAR werden als Individualisierte Befragungen durchgeführt. Dies sind Befragungen und andere Datenerhebungen, bei denen es vorgesehen ist, dass die Antworten der Teilnehmer und Ihre sonstigen im Rahmen der Befragung erhobenen Daten an KANTARs Auftraggeber oder weitere den Teilnehmern gegenüber kommunizierte Dritte auf individueller Ebene (d.h. personenbezogen) weitergeleitet werden sollen. KANTARs Auftraggeber erhalten das Feedback der Teilnehmer (z.B. zu ihren Produkten und Services) also direkt und auf Einzelfallebene und haben dadurch wiederum die Möglichkeit, sich damit zu befassen, ihre Produkte und Services zu verbessern und gegebenenfalls auf die Teilnehmer zurückzukommen.

  KANTAR hält bei der Durchführung Individualisierter Befragungen sämtliche anwendbaren gesetzlichen Bestimmungen (insbesondere die DSGVO) ein. Daneben hält Kantar den von ESOMAR herausgegebenen internationalen ICC-ESOMAR-Kodex ein. Weitere Informationen hierzu finden sich unter https://www.esomar.org/what-we-do/code-guidelines.

  Die Individualisierten Befragungen sind durch technische und organisatorische Maßnahmen von Studien der Markt- und Sozialforschung getrennt. Dies gilt natürlich auch für die insoweit verarbeiteten Daten. Eine Abgrenzung erfolgt auch auf Ebene der Datenschutzerklärungen.

- KANTAR arbeitet im Einklang mit sämtlichen anwendbaren Gesetzen. Neben der DSGVO werden, soweit anwendbar, insbesondere das BDSG-neu, das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG) und die wettbewerbsrechtlichen Vorschriften, insbesondere § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), beachtet.

## 3.3 Einzelheiten der Verarbeitung

### 3.3.1 Kategorien betroffener Personen und personenbezogener Daten

- Studienteilnehmer im Rahmen der Markt- und Sozialforschung (Selbst nach mathematischen Zufallsverfahren erzeugte oder von Auftraggebern, Adresshändlern, Einwohnermeldeämtern bereitgestellte Haushalts- und Unternehmensadressen / Telefonnummern, Befragungsdaten, ggf. weitere Angaben, sofern diese zur Erfüllung des jeweiligen Zwecks erforderlich sind)
- Bewerber sowie bestehende und ehemalige Beschäftigte von KANTAR (insbesondere Kontaktdaten. Gehaltsrelevante Daten, Gehaltseinordnung, Organisatorische Zuordnung, Perfomance-Daten, Zeitwirtschaftsdaten, Gesundheitsdaten, Vermögensbildung)
- (Potentielle) Kunden und Lieferanten (insbesondere Adressdaten, Identifikationsdaten, Vertragsdaten, Interessengebiete, Angebotsdaten, Steuerungsdaten, ggf. sonstige Daten, soweit sie für die ordnungsgemäße und sachgerechte Abwicklung der Geschäftsbeziehung erforderlich sind, z.B. Abrechnungsdaten)

### 3.3.2 Kategorien von Empfängern mit Zugriff auf personenbezogene Daten

Externe Dienstleister im Rahmen der Auftragsverarbeitung nach Art. 28 DSGVO, Gesellschaften des Kantar-Konzerns und interne Stellen / Fachabteilungen von KANTAR zur Erfüllung des jeweiligen Zwecks, sowie öffentliche Stellen bei Vorliegen entsprechender Vorschriften.

Die Ergebnisse aus sämtlichen Studien der Markt-, Meinungs- und Sozialforschung werden ausschließlich in anonymisierter Form ausgewertet und nur anonymisiert an Dritte weitergegeben.

Bei Individualisierten Befragungen können mit Einverständnis des Betroffenen personenbezogene Daten an Kunden und Dritte gegeben werden.

### 3.3.3 Zugriffsberechtigte Personengruppen

Es haben nur diejenigen Mitarbeiter Zugriff auf die Daten, die für die Erfüllung des jeweiligen Zwecks erforderlich sind.

### 3.3.4 Geplante Datenübermittlung in Drittstaaten

Eine Übermittlung in Länder außerhalb der Europäischen Union (EU) / des Europäischen Wirtschaftsraums (EWR) erfolgt nur im Rahmen einer Auftragsverarbeitung, im Rahmen eines berechtigten Interesses oder aufgrund einer freiwilligen und informierten Einwilligung der jeweils Betroffenen.

Die Übermittlung erfolgt zudem nur nach Maßgabe der gesetzlichen Zulässigkeitsvorschriften gemäß Artt. 44 ff. DSGVO.

### 3.3.5 Regelfristen für die Löschung personenbezogener Daten

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden personenbezogenen Daten routinemäßig gelöscht. Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, sobald der jeweilige Zweck erfüllt ist.

# 4. Technische und Organisatorische Maßnahmen

KANTAR hat nach den Vorgaben des Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen sind dokumentiert und werden fortwährend gepflegt.

Im Übrigen verfügt KANTAR über das ISO 27001-Zertifikat für den Geltungsbereich Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse.

| **1. Pseudonymisierung, Artt. 32 (1) a) DSGVO, 25 I DSGVO** | **Maßnahmen** |
|---|---|
| Einsatz von Pseudonymisierungsverfahren | Trennung von Adress- und Befragungsdaten. Verbindung beider erfolgt über systematische IDs. Die Speicherung erfolgt weitestmöglich getrennt voneinander<br><br>Berechtigungskonzept für den Zugriff auf die IDs nach Need-to-know<br><br>Adressdaten werden verschlüsselt übertragen. |
| **2. Verschlüsselung personenbezogener Daten, Art. 32 (1) a) DSGVO** | **Maßnahmen** |
| Gesicherter Adressaustausch | Zentrales Portal für die Adresslieferung nach und von Extern; Up- und Download verschlüsselt<br><br>Richtlinie für zulässige Verfahren zur Übertragung vertraulicher Informationen (einschließlich personenbezogener Daten) |
| Verschlüsselung von E-Mails | Vertrauliche E-Mails werden mittels AES256 verschlüsselt (End-to-End); Mail-Domain: Transportverschlüsselung aktiviert |
| Verschlüsselung von Datenträgern | Verschlüsselung der Laptop-Festplatten<br><br>Hardwareverschlüsselte USB-Sticks |
| Remotezugriff | Remotezugriff und Fernwartung ausschließlich mittels verschlüsselter Verbindungen |

| | |
|---|---|
| Gesicherter Transport physischer Datenträger (z.B. abgeschlossener Transportcontainer) | Backup-Bänder werden durch IT-Dienstleister in einem abgeschlossenen Transportbehältnis in eine geschützte Lokation ausgelagert |
| Gesichertes W-LAN | WPA2 PSK mit Kennwort |
| Verschlüsselung bei der Bereitstellung von Online-Diensten | SSL (https) TLS 1.2/1.3; Leitlinie zum Einsatz kryptografischer Techniken |
| Verschlüsselung von Projektlaufwerken | Nach Bedarf: End-to-End-Verschlüsselung vertraulicher Projektverzeichnisse und -ordner (Verschlüsselungssoftware von Tetraguard) |
| Mobile Endgeräte | Verschlüsselung aller mobilen Endgeräte |
| **3. Fähigkeit, die Vertraulichkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, Art. 32 (1) b) DSGVO** | **Maßnahmen** |
| **3.1 Zutrittskontrolle (Verhinderung des Zutritts Unbefugter zu DV-Anlagen mit personenbezogenen Daten)** | |
| Gebäude- / Etagensicherung | Besetzter Empfang / an größeren Standorten getrennte kontrollierte Zugänge für Mitarbeiter und Lieferanten<br><br>Zutrittskontrollsystem, mehrstufiges Sicherheitssystem<br><br>Gebäude außerhalb der Dienstzeiten verschlossen<br><br>Wachdienst außerhalb der Dienstzeit<br><br>Trennung von Bearbeitungs- und Publikumszonen<br><br>Zutritt zu den einzelnen Etagen nur mit elektronischem Chip<br><br>Gesondert gesicherter Zutritt zum Rechenzentrum und zu den Serverräumen<br><br>Schlüsselregelung<br><br>Anweisung zur Ausgabe von Schlüsseln<br><br>Begleitung von Besucherzutritten durch eigene Mitarbeiter<br><br>Einbruchalarm und/oder Bestreifung des Gebäudes durch Wachdienst |

| | |
|---|---|
| Protokollierung und Kontrollierung des Gebäudezutritts | Elektronische Zutrittskontrolle (Chip) für alle Mitarbeiter<br><br>Nachvollziehbarkeit des Zutritts zum Gebäude / zu den Etagen<br><br>Besucherausweise |
| Einrichtung des Rechenzentrums als Sicherheitsbereich | Zentrale Server sind in einem verschlossenen Rechenzentrum mit Zugangskontrolle (geloggter Zutritt) und Einbruchs-, Brandmelde- und Löschanlage untergebracht |
| | Dezentrale Server an den Standorten sind in mitEinbruch- und Brandmeldeanlagen ausgestatteten Technikräumen verschlossen<br><br>Einbruch- und Brandmeldeanlagen sind auf externen Wachdienst aufgeschaltet<br><br>Aufbewahrung von Sicherungsmedien im Safe in geschützter Lokation<br><br>Schließanlage: Schlüsselregelung für Zutrittsberechtigte |
| Festlegung zutrittsberechtigter Personen | Protokollierung der Chip- / Schlüsselausgabe<br><br>Sonderzutrittsregelungen für Sonstige: nur in Begleitung Zutrittsberechtigter<br><br>Protokollierung des Zugangs |
| Sicherung der Netzwerke | Verteilerkästen sind vor unbefugtem Zugriff abgesichert<br><br>24 x 7 Netzwerk-Management wird zentral in Verantwortung durch IT-Dienstleister durchgeführt<br><br>Router, Switches und Netzwerkkomponenten sind in verschlossenen Räumen oder Stahlbehältnissen untergebracht<br><br>Verkabelungen befinden sich in geschlossenen Kabelschächten; Verkabelung ist dokumentiert |
| **3.2 Zugangskontrolle (Verhinderung der Nutzung von DV-Systemen mit personenbezogenen Daten durch Unbefugte)** | |

| | |
|---|---|
| Internes Legitimationsverfahren für Benutzercodes betreffend Dateien und Systeme / Dokumentiertes organisatorisches Verfahren für: | |
| Vergabe, Sicherung, Änderung, Löschung von Benutzer-Accounts | Benutzer-Accounts mit individualisierten Zugangsrechten<br><br>Bei Neueinstellungen erhält Kantars IT-Dienstleister von HR automatisiert und dokumentiert die für den Netzbetrieb relevanten |
| | Personaldaten (Mitarbeiterkürzel, Mitarbeiternummer, Kostenstelle, Eintrittsdatum) |
| Benutzer-Accounts ausgeschiedener Mitarbeiter | Bei Versetzung / Ausscheiden eines Mitarbeiters dokumentierter Vorgang des Entzugs von Zugangsberechtigungen<br><br>Individuelle Benutzer-Accounts werden dokumentiert gesperrt / gelöscht |
| Protokollierung des Zugriffs auf Anwendungen und Systeme | Nach Bedarf und Applikation rückwirkend für mehrere Monate |
| Policy für Login und PW | Security Policy<br><br>Globale Passwort-Policy<br><br>Mindestlänge von Benutzercodes: 5 Zeichen<br><br>Passwortmindestlänge: 8 Zeichen<br><br>Passwort Komplexität (Sonderzeichen, Ziffern,Groß- / Kleinschreibung) vorgeschrieben<br><br>Ausschluss von Trivialpasswörtern<br><br>Erzwungener Passwortwechsel nach 60 Tagen<br><br>Bei Passwortverlust dürfen Passwörter nur von IT nach eindeutiger Authentifikation zurückgesetzt werden<br><br>Passwort History / alte Passwörter dürfen nicht wiederverwendet werden (10 Generationen) |
| Automatisches Sperrsystem bei fehlerhaft eingegebenen Benutzercodes / Passwort | Sperrung des Zugangs bei mehr als vier fehlerhaften Anmeldeversuchen |

| | |
|---|---|
| Automatische / manuelle Tastatur- und Bildschirmsperre bei Nichtnutzung / Abwesenheit | Standardmäßige Einrichtung der PC<br><br>Automatische Tastatur- und Bildschirmsperre 10 Minuten nach letztem Gebrauch<br><br>Manuelle Sperre bei Verlassen des Arbeitsplatzes / Clean Desk Policy<br><br>Aufhebung der Sperre nur durch Eingabe eines Passworts |
| **3.3 Zugriffskontrolle (Verhinderung des Zugriffs auf oder der Veränderung personenbezogener Daten durch Unbefugte)** | |
| Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte | Differenziertes Berechtigungssystem für den Zugriff auf Dateien, System- und Anwendungsprogramme durch Zugangsberechtigte (inklusive Wartungsberechtigte)<br><br>Vergabe von einzelnen, den Funktionen entsprechenden Rollen und Rechten durch Kantars IT-Dienstleister nach Freigabe durch den Vorgesetzten<br><br>Zugriff auf Netzlaufwerke für berechtigte Benutzer(gruppen)<br><br>Differenzierte Berechtigungen für lesenden und schreibenden (Änderung / Löschung) Zugriff<br><br>Userrechte werden anwendungsbezogen vergeben<br><br>Anwendungsbezogene Protokollierung, welche Benutzer auf die Datenbestände zugreifen<br><br>Aufbewahrung der Zugriffsprotokolle 6 Monate rückwirkend für sicherheitsrelevante Daten |

| | |
|---|---|
| Datenträger / Datenträgerverwaltung | Nachweis über Eingang, Ausgang sowie Bestand<br><br>Lagerung der Datenträger im internen Sicherheitsbereich<br><br>Stets in verschlossenen Räumen / Safe<br><br>Dokumentierte Sicherungsverfahren<br><br>Festlegung berechtigter Personen<br><br>Verbot des Einsatzes privater Datenträger |
| Kontrollierte Vernichtung von Datenträgern | Vernichtung von Adressdaten erfolgt nach gemäß ISO 9001 festgelegten Prozessbeschreibungen<br><br>Datenvernichtung nach DIN 66399 (Sicherheitsstufe P3, Schutzklasse 2) (physische |
| | Zerstörung) über zertifizierten Entsorger nach Terminabsprache<br><br>Verwendung von Datenschutztonnen oder Schreddern (Sicherheitsstufe P5)<br><br>Nicht mehr zu verwendende Fest- und Wechselplatten werden von IT unbrauchbar gemacht<br><br>Verwahrung von Datenträgern bis zur Entsorgung in einem separaten, zugangsgesicherten Hardware-Archiv<br><br>Vorhalten von Entsorgungsbescheinigungen |
| Gesonderte Regelungen für mobile Endgeräte | Mobile PC (Laptops, Notebooks) sind gesichert via Kensington-Lock und werden außerhalb der Arbeitszeiten unter Verschluss aufbewahrt<br><br>Festplattenverschlüsselung auf allen Laptops und mobilen Geräten |
| **3.4 Trennungskontrolle (Gewährleistung getrennter Verarbeitung zu unterschiedlichen Zwecken erhobener personenbezogener Daten)** | |

| | |
|---|---|
| Getrennte Bearbeitung / Dateiverwaltung jedes Auftrags | Sichergestellt über Prozessbeschreibungen undPrüfungsanweisungen gem. ISO-zertifiziertem Qualitätsmanagement-System<br><br>Trennung über Projektnummer<br><br>Daten werden nur zum vereinbarten Zweck genutzt / verarbeitet |
| Getrennte Protokollierung der einzelnen Arbeitsschritte bei jedem Auftrag | Sichergestellt über Prozessbeschreibungen undPrüfungsanweisungen gem. ISO-zertifiziertem Qualitätsmanagement-System |
| Funktionstrennung | Speicherung von Daten und Programmen in unterschiedlichen Verzeichnissen<br><br>Pseudonymisierung von Testdaten |
| **4. Fähigkeit, die Integrität der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, Art. 32 (1) b) DSGVO** | **Maßnahmen** |
| **4.1 Weitergabekontrolle (Verhinderung unbefugten Lesens, Kopierens, Veränderns oder Entfernens personenbezogener Daten während der elektronischen Übertragung / des Transports / der Speicherung)** | |
| Datenweitergabe | Weitergabe von Dateien nur an berechtigte Personen mit Weitergabeprotokoll<br><br>Dokumentation aller Adressen im Rahmen der Weitergabekette<br><br>Vollständigkeits- und Korrektheitskontrolle |

| | |
|---|---|
| Transportsicherung | Interne Weitergabe: über internes Netzwerk / gesichertes Austauschportal<br><br>Teilnehmerkreis des Portals ist durch Benutzerkennung und Rechtekonzepte reglementiert<br><br>Nachweis der Zugriffs- und Weitergabekontrolle durch Log-Files<br><br>Externe Weitergabe: verschlüsselt in Absprache mit dem Empfänger und / oder per Kurier<br><br>Komprimiert / Verschlüsselt mit Passwortschutz, starker Verschlüsselungsalgorithmus (Standard: AES-256)<br><br>Verschlossene Transportbehälter<br><br>Zuverlässige Boten / Transportunternehmen |
| **4.2 Eingabekontrolle (Nachträgliche Prüfmöglichkeit darüber, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben / verändert / entfernt wurden)** | |
| Protokollierungs- und Protokollauswertungssysteme | Systemunterstütze Protokollierung der Dateinutzung / Dateiveränderung<br><br>Auswertbarkeit von Protokollen rückwirkend (6 Monate) für sicherheitsrelevante Daten |
| Dokumentation der Eingabeverfahren | Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten |
| | Nachträgliche Nachvollziehbarkeit der erfolgten Datenveränderungen |
| **5. Fähigkeit, die Verfügbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, Art. 32 (1) b) DSGVO** | **Maßnahmen** |

| | |
|---|---|
| Datensicherungskonzept | Zentrales Backup-System mit Berechtigungs- und Löschkonzept<br><br>Durchführung der Datensicherungsmaßnahmen durch IT-Dienstleister<br><br>Veränderte Datenbestände werden mind. täglich gesichert (via Band oder Snap-Shot Technologie)<br><br>Für Wochentage wird ein eigenes Bandset genutzt<br><br>Wöchentlich werden alle Datenbestände voll gesichert<br><br>Monatliche Überprüfung der Sicherungsverfahren<br><br>Tägliche Überprüfung der Sicherungsprotokolle<br><br>Monatliche Test-Restores für Daten<br><br>Restore durch IT-Dienstleister<br><br>Aufbewahrung der Backup-Kopien in unterschiedlichen feuergeschützten und abgeschlossenen Räumen / Safes<br><br>Richtlinien zur Datenarchivierung<br><br>Notfallpläne / IT Continuity Management<br><br>IT Continuity Test nach festgelegten Prozessen und Zeitintervallen |
| Brandschutzeinrichtungen | Brandabschnitte<br><br>Brandschutztüren<br><br>Klimatisierung von Server- / Technikräumen<br><br>Rauch- und Brandmelder im Rechenzentrum |
| | Koppelung des Rechenzentrums mit Notrufzentrale<br><br>Feuerlöschanlage im Rechenzentrum München, Sprinkleranlage im Rollregallager München<br><br>Flucht-, Rettungs- und Brandschutzpläne |

| | |
|---|---|
| Softwareinstallation | Laptops/PC werden mit Standardsoftware ausgestattet<br><br>Ergänzung der Standardsoftware nur nach Prüfung und Freigabe durch CIO |
| Firewall-Installation | Schutz des internen Netzwerks durch mehrereFirewall-Systeme<br><br>Next-Generation Firewall - (NGFW) - Palo Alto Networks<br><br>Intrusiondetection (IDS)<br>Intrusionprevention (IPS) im Einsatz<br><br>Eingehende Mails werden mit einem automatisierten Verfahren auf schadenstiftende Software untersucht (SPAM-Filter) |
| Datenträger | Erhaltene oder auszuliefernde Datenträger werden mit einem Virenscanner auf schadenstiftende Software hin überprüft, bevor sie verwendet oder versendet werden |
| Virenschutz | Mehrstufiger Virenschutz. Installation und ständige Aktualisierung von automatischem Virenschutz |
| Sperrung von Sites | Sperrung indizierter Websites |
| Stromversorgung | USV-Systeme und Notstromdiesel an Großlokationen (gesichertes Herunterfahren der Server bei Stromausfall) |
| Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates | Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).<br><br>Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden. |

| | |
|---|---|
| | Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.<br><br>Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.<br><br>Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen<br><br>Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen. |
| **6. Fähigkeit, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen, Art. 32 (1) b) DSGVO** | **Maßnahmen** |
| Kontrolle von Verfügbarkeit und Performance | Server- & Application Monitoring: Überwachung der Produktivsysteme, Speicherkapazitäten<br><br>Vorauswahl entsprechender Performance-Indikatoren inklusive regelmäßiger Überprüfung<br><br>Langzeitauswertung rückwirkend und vorausschauend und Ableitung entsprechender Maßnahmen |
| **7. Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, Art. 32 (1) c) DSGVO** | **Maßnahmen** |
| Backup-Konzept (unter Festlegung der Häufigkeit, der eingesetzten Backup-Medien, Aufbewahrungsfrist und Ort) | Policy und Prozedur werden jährlich geprüft und erneuert<br><br>Durchführung monatlicher Restore-Tests |
| Redundante Datenhaltung | VMWare Fail-Over-Cluster, Multiredundante SAN |
| **8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur** | **Maßnahmen** |
| **Gewährleistung der Sicherheit der Verarbeitung, Art. 32 (1) d) DSGVO** | |

| | |
|---|---|
| **8.1 Auftragskontrolle (Gewährleistung, dass die Verarbeitung personenbezogener Daten im Rahmen der Auftragsverarbeitung nur entsprechend den Weisungen des Auftraggebers erfolgt)** | |
| Formalisierung der Auftragsvergabe zwischen den Hauptvertragsparteien | Detaillierte schriftliche Regelung der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes<br><br>Eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten<br><br>Dokumentation der Prozessschritte über interne Systeme<br><br>Kontrolle der Arbeitsschritte<br><br>Verwaltung, Sicherung und Dokumentation der Adressdaten in dem dafür bereitgestellten Interaktionssystem |
| Formalisierung der Auftragsvergabe gegenüber sämtlichen Unterauftragnehmern | Sorgfältige Auswahl der Auftragnehmer<br>Detaillierte schriftliche Regelung der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes<br><br>Verpflichtung der Subunternehmer auf Datenschutz, Geheimhaltung und Informationssicherheit<br><br>Vereinbarung von Auftragsverarbeitungsverträgen und Festlegung technischer und organisatorischer Maßnahmen mit Auftragsverarbeitern<br>Auftragskontrolle und Dokumentation |
| **8.2 Datenschutz-Management, Incident-Response-Management und Datenschutzfreundliche Voreinstellungen** | |
| Datenschutz-Organisation | Lokale interne Datenschutzabteilung mit bestelltem Datenschutzbeauftragten<br><br>Anbindung an Konzern-Datenschutz-Organisation für die europäischen Kantar-Gesellschaften<br><br>Projektübergreifende Verarbeitungsverzeichnisse und |

| | |
|---|---|
| | Datenschutzfolgenabschätzungen, ergänzt durch Pflichtangaben zum Datenschutz für jede neue Projektanlage<br><br>Sicherheitskonzept i.R.v. ISO 27001<br><br>Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen<br><br>ISO27001-Zertifizierung einschließlich interner und externer Audits<br><br>Konzerninterne Datenschutz-Audits<br><br>Nachweisbare Verpflichtung der Mitarbeiter auf Datenschutz und Vertraulichkeit |
| Incident-Response-Management und Wahrung der Betroffenenrechte | Prozess zur Bearbeitung von Anfragen zur Geltendmachung von Betroffenenrechten<br><br>Vorfallsreaktionsplan und Policy zur Meldung von Datenschutzvorfällen |
| Dokumentierte periodische Schulungen/Trainings und Sensibilisierungskampagnen innerhalb der Organisation | Regelmäßige Schulungen/Trainings der Mitarbeiter zum Datenschutzrecht<br><br>Regelmäßige Schulungen/Trainings der Mitarbeiter zu Daten- und Informationssicherheit (einschließlich zu Verhaltensweisen im Geschäftsalltag)<br><br>Gesonderte Sensibilisierungskampagnen und Schulungen zu bestimmten Fragestellungen aus dem Datenschutz und der Daten- und Informationssicherheit |
| Implementierung datenschutzfreundlicher Voreinstellungen, Art. 25 Abs. (2) DSGVO | Automatisierte Abfrage von Pflichtangaben zum Datenschutz bei jeder neuen Projektanlage<br><br>Lokale interne Datenschutzabteilung zur Beratung der Mitarbeiter bei der datenschutzkonformen Anlage von Projekten und der Einführung neuer Anwendungen und Prozesse<br><br>Policies und Arbeitsanweisungen zur frühzeitigen Einbindung der Datenschutzabteilung bei der Entwicklung neuer Prozesse |

# 5. Zertifikate

siehe Folgeseiten

# ZERTIFIKAT

KANTAR

## ISO 9001:2015

DEKRA Certification GmbH bescheinigt hiermit, dass die Organisation

**Kantar GmbH**

**Zertifizierter Bereich:**

Markt-, Meinungs- und Sozialforschung

**Zertifizierter Standort:**

Landsberger Straße 284, 80687 München, Deutschland
(weitere Standorte siehe Anhang)

ein Qualitätsmanagementsystem entsprechend der oben genannten Norm eingeführt hat und aufrechterhält. Der Nachweis wurde mit Auditbericht-Nr. A20071257_1 erbracht.

| | | | |
|---|---|---|---|
| Zertifikats Registrier-Nr.: | 90103074/7 | Zertifikat gültig vom: | 27.02.2021 |
| Gültigkeit vorheriges Zertifikat: | 26.02.2021 | Zertifikat gültig bis: | 26.02.2024 |

DEKRA Certification GmbH, Handwerkstraße 15, 70565 Stuttgart

Dr. Gerhard Nagel
DEKRA Certification GmbH, Berlin, 25.01.2021

DAkkS Deutsche Akkreditierungsstelle D-ZM-16029-01-01

# Anhang zum Zertifikat Nr. 90103074/7

gültig vom 27.02.2021 bis 26.02.2024

Die folgenden Standorte / Firmen fallen unter das o.g. Zertifikat:

| | Zentrale | Zertifizierter Standort | Zertifizierte Bereiche |
|---|---|---|---|
| | Kantar GmbH | Landsberger Straße 284<br>80687 München<br>Deutschland | Markt-, Meinungs- und Sozialforschung |
| | **an den folgenden Standorten / bei den Firmen an den folgenden Standorten** | | **Zertifizierte Bereiche** |
| 1. | Kantar GmbH | Darmstädter Landstraße112<br>D-60598-Frankfurt am Main | Markt-, Meinungs- und Sozialforschung; |
| 2. | Kantar GmbH | Thumenberger Weg 27<br>D-90494 -Nürnberg, | Markt-, Meinungs- und Sozialforschung |
| 3. | telquest GmbH | Ludwigsluster Straße 29<br>D-19370-Parchim | Telefonische Datenerhebung |

Dr. Gerhard Nagel
DEKRA Certification GmbH, Berlin, 25.01.2021

# ZERTIFIKAT

KANTAR

## ISO 20252:2019

DEKRA Certification GmbH bescheinigt hiermit, dass die Organisation

**Kantar GmbH**

**Zertifizierter Bereich:**

Markt-, Meinungs- und Sozialforschung

**Zertifizierter Standort:**

Landsberger Straße 284, 80687 München, Deutschland
(weitere Standorte siehe Anhang)

die Anforderungen der ISO 20252:2019 Markt-, Meinungs- und Sozialforschung erfüllt. Der Nachweis wurde im Rahmen des Zertifizierungs-Audits Bericht-Nr. A20071257_1 erbracht. Dieses Zertifikat bestätigt, dass das QM-System die weiterreichenden Anforderungen der ISO 20252:2019 gegenüber der ISO 9001:2015 erfüllt. Dieses Zertifikat ist nur in Verbindung mit der erfolgreichen Durchführung der Überwachungsaudits gültig. Dieses Zertifikat gilt nur in Verbindung mit dem Hauptzertifikat Nr. 90103074/7.

| | | | |
|---|---|---|---|
| Zertifikats Registrier-Nr.: | 3004078001/6 | Zertifikat gültig vom: | 27.02.2021 |
| Gültigkeit vorheriges Zertifikat: | 26.02.2021 | Zertifikat gültig bis: | 26.02.2024 |

Qualitätsmanagement in der Markt- und Sozialforschung ISO 20252 DEKRA zertifiziert

Dr. Gerhard Nagel
DEKRA Certification GmbH, Berlin, 25.01.2021

DEKRA Certification GmbH * Handwerkstraße 15 * D-70565 Stuttgart * www.dekra.de/audits

Seite 1 von 2

# Anhang zum Zertifikat Nr. 3004078001/6

gültig vom 27.02.2021 bis 26.02.2024

Die folgenden Standorte / Firmen fallen unter das o.g. Zertifikat:

| | **Zentrale** | **Zertifizierter Standort** | **Zertifizierte Bereiche** |
|---|---|---|---|
| | Kantar GmbH | Landsberger Straße 284<br>80687 München<br>Deutschland | Markt-, Meinungs- und Sozialforschung |
| | **an den folgenden Standorten / bei den Firmen an den folgenden Standorten** | | **Zertifizierte Bereiche** |
| 1. | Kantar GmbH | Darmstädter Landstraße112<br>D-60598-Frankfurt am Main | Markt-, Meinungs- und Sozialforschung |
| 2. | Kantar GmbH | Thumenberger Weg 27<br>D-90494 -Nürnberg, | Markt-, Meinungs- und Sozialforschung |

Dr. Gerhard Nagel
DEKRA Certification GmbH, Berlin, 25.01.2021

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

# ZERTIFIKAT

**Die Zertifizierungsstelle**
**der TÜV SÜD Management Service GmbH**

bescheinigt, dass das Unternehmen

## KANTAR

**Kantar GmbH**
Landsberger Str. 284
80687 München
Deutschland

für den Geltungsbereich

**Umgang mit Daten und Informationen**
**im Rahmen der Markt- und Sozialforschungsprozesse**

**einschließlich der Standorte und Geltungsbereiche**
**gemäß Anlage**

ein Informationssicherheitsmanagementsystem
gemäß „Erklärung zur Anwendbarkeit" eingeführt hat und anwendet.

Durch ein Audit, Auftrags-Nr. **70763550**,
wurde der Nachweis erbracht, dass die Forderungen der

## DIN EN ISO/IEC 27001:2017

erfüllt sind.

Dieses Zertifikat ist gültig vom **30.03.2021** bis **29.03.2024**.

Zertifikat-Registrier-Nr.: **12 310 46872 TMS**.

Version der Erklärung zur Anwendbarkeit: **v2.7, 21.01.2021**.

Leiter der Zertifizierungsstelle
München, 31.03.2021

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

Seite 1 von 2

TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

TÜV®

MS/01-01/2019

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Management Service

# Anlage zur Zertifizierungsurkunde Nr.: 12 310 46872 TMS

| Standorte | Geltungsbereich |
|---|---|
| **Kantar GmbH**<br>Landsberger Str. 284<br>80687 München<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Kantar GmbH**<br>Alt-Moabit 96 a<br>10559 Berlin<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Kantar GmbH**<br>Stieghorster Str. 86-90<br>33605 Bielefeld<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Kantar GmbH**<br>Darmstädter Landstr. 112<br>60598 Frankfurt<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Kantar GmbH**<br>Friedensallee 11<br>22765 Hamburg<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Kantar GmbH**<br>Thumenberger Weg 27<br>90491 Nürnberg<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **Infratest dimap**<br>**Gesellschaft für Trend- und Wahlforschung mbH**<br>Alt-Moabit 96 a<br>10559 Berlin<br>Deutschland | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |
| **TNS Infratest Slovakia s.r.o.**<br>Business Center, II Blok E, 5. posch, Prievozska 4<br>821 09 Bratislava<br>Slowakische Republik | Umgang mit Daten und Informationen im Rahmen der Markt- und Sozialforschungsprozesse |

IAF

DAkkS Deutsche Akkreditierungsstelle D-ZM-14143-01-00

Leiter der Zertifizierungsstelle
München, 31.03.2021



TÜV SÜD Management Service GmbH • Zertifizierungsstelle • Ridlerstrasse 57 • 80339 München • Germany
www.tuev-sued.de/certificate-validity-check

TÜV®

MS/01-01/2019