Leitfaden Datenschutz und Qualitätssicherung bei Mitarbeitendenbefragung für teilnehmende Personen

Angaben zur Durchführung

Für die Durchführung von Befragungen hat sich die VisionGesund den folgenden Qualitätsstandards und Datenschutzobliegenheiten verpflichtet.

1 Qualitätsstandards für Befragungsprojekte

Die Durchführung und Auswertung von Mitarbeitendenbefragungen durch VisionGesund orientiert sich insbesondere an folgenden Qualitätsstandards:

- Standards für Qualitätssicherung des ADM
- Richtlinie für Befragungen (Zusammenarbeit von ADM, ASI, BVM und DGOF)

2 Sicherung der Anonymität

VisionGesund hat sich den Vorgaben der DSGVO und des BDSG auch im Hinblick auf Befragungsprojekte verpflichtet. Das Anliegen ist es, den Schutz und die Anonymität der erhobenen Daten zu gewährleisten. Im Sinne der beiden Rechtsnormen werden Teilnehmer:innen einer Befragung durch die Datenerhebung nicht in ihrem Persönlichkeitsrecht eingeschränkt. Folgende Punkte werden deshalb bei der Datenerhebung und -verarbeitung berücksichtigt:

Datenaufnahme

Bei Mitarbeitendenbefragungen und Evaluationsmaßnahmen garantiert VisionGesund den Mitarbeiter:innen vollständige Anonymität. Personenbezogene Daten, wie z. B. Name, Vorname, E-Mail-Adresse werden bewusst nicht erhoben, um einen späteren Rückschluss auf personenbezogene Einzeldaten zu vermeiden und die Datensicherheit zu gewährleisten. Zudem weist VisionGesund ausdrücklich darauf hin, dass Teilnehmer:innen von Befragungen alle Daten auf freiwilliger Basis abgeben und keinerlei externen Zwängen unterliegen. Auch pseudonyme Daten werden nicht erhoben (hier insbesondere: IP-Adresse und Cookies bei Online-Umfragen, näheres im folgenden Kapitel *Datenschutz der Plattformen für Online-Umfragen*).

Erhebung soziodemographischer Merkmale

Im Rahmen der von VisionGesund durchgeführten Mitarbeitendenbefragungen werden nur dann soziodemographische Merkmale abgefragt, wenn Sie dem Ziel der Befragung dienen. Dies muss vom Auftraggeber explizit angefordert werden. Mithilfe dieser Variablen ist es möglich, Sachverhalte für bestimmte Zielgruppen spezifisch aufzudecken (Zielgruppenspezifität). Um die Anonymität zu gewährleisten, werden daher:

- Namen und Adressen grundsätzlich nicht erhoben.
- Personenmerkmale wie Alter oder Geschlecht regelmäßig nicht erhoben, außer der/die Auftraggeber:in wünscht dies explizit.

Dann gilt: Auswertungen nach Alter und Geschlecht werden nicht mit weiteren demographischen Merkmalen zusammen ausgewertet (Kreuzauswertung), um die Anonymität zu wahren und Ergebnisse höchstens auf ein Merkmal zusammenzufassen.

- Nur die für die Zielsetzung der Befragung notwendigen soziodemographischen Variablen abgefragt (so viele wie nötig, so wenig wie möglich, z. B. hauptsächlicher Tätigkeitsbereich oder Standort).

Zugang zur Online-Befragung

Der anonymisierte Zugang zu Online-Befragungen wird durch Rubbelkarten mit Zugangscodes gewährleistet. Hierzu lässt VisionGesund Rubbelkarten mit vierstelligen Zugangscodes produzieren (Zahlen- und/oder Buchstabenkombination), die durch den/die Auftraggeber:in an die Mitarbeiter:innen verteilt werden. Nur mit gültigem Zugangscode kann an der Befragung teilgenommen werden. Dabei ist der Code so lange nicht sichtbar, bis er von den Mitarbeiter:innen zur eigenen Verwendung freigerubbelt wird. VisionGesund und Auftraggeber:in können die Codes keiner Person zuordnen und können keinen Einfluss darauf nehmen, wer welchen Code bekommt (doppelblinde Zuordnung). Darüber hinaus kann eine anonyme Zuordnung von Dummy-E-Mail-Adressen zum Versand der Zugangscodes genutzt werden: Hierzu müssen durch den/die Auftraggeber:in randomisierte, pseudonyme E-Mail-Adressen erzeugt und VisionGesund in einfacher tabellarischer Form zur Verfügung gestellt werden. VisionGesund erstellt anschließend zufallsgenerierte Zugangscodes, welche per Serienbrieffunktion über die E-Mail-Dummys an die Teilnehmer:innen versandt werden.

Werden Zugangscodes per EXCEL-Liste bereitgestellt, wird sichergestellt, dass durch den/die Auftraggeber:in eine interne Verteilung der Codes erfolgt, ohne dass VisionGesund darüber in Kenntnis gesetzt wird, welche Person welchen Code erhält. Durch die Trennung dieser Informationen bleibt die Anonymität erhalten.

Nutzung der Daten

Erhobene Angaben werden ausschließlich zur Auswertung des Fragebogens genutzt. Die Daten des Fragebogens sind alleinig durch die Projektmitarbeiter:innen von VisionGesund einsehbar und bearbeitbar. Erhebung, Einsicht und Nutzung der Daten richten sich dabei nach Art. 5, 24, 29 und 32 DSGVO. Das Datengeheimnis wird zu jeder Zeit gewahrt.

Auswertung der Daten

Alle erhobenen Daten werden ausschließlich anonymisiert und in zusammengefasster Form ausgewertet und statistisch dargestellt. Die Ergebnisse werden so ausgewertet, dass sie einen Rückschluss auf einzelne Personen nicht zulassen. Es werden keine Auswertungen von Bereichen insgesamt oder Fragen im Speziellen vorgenommen, solange die Fallzahl n<5 beträgt. Die Größe des n wird maßgeblich durch den/die Auftraggeber:in bestimmt und kann nach oben angepasst werden (z. B. kleinstes n=10). *Beispiele zur Verdeutlichung: Sollten nur n=3 Teilnehmer:innen sich dem Tätigkeitsbereich A zuordnen, wird Tätigkeitsbereich A nicht separat ausgewertet. Sollten sich insgesamt 5 Personen dem Tätigkeitsbereich A zuordnen, einzelne Fragen jedoch nicht von allen Teilnehmer:innen beantwortet werden, entfällt die Auswertung für diese einzelnen Fragen.*

Auskunft, Sperrung oder Löschung Ihrer Daten

VisionGesund hat keine Möglichkeit, erhobene Daten zurückzuverfolgen, daher ist es VisionGesund im Nachgang auch nicht möglich, Auskunft über die erhobenen Daten zu erteilen, diese zu sperren oder personenbezogen zu löschen.

Löschung des Datensatzes

Der Datensatz wird zur Auswertung verschlüsselt auf den Datenträgern von VisionGesund gespeichert. Auf Verlangen des/der Auftraggeber:in erfolgt eine Löschung aller Rohdatensätze aus der Mitarbeitendenbefragung nach Abschluss des vereinbarten Projektzeitraums die projektverantwortlichen Mitarbeitenden.

Die Ergebnisberichte werden verschlüsselt auf den Datenträgern von VisionGesund archiviert. Spätestens mit Beendigung der vertraglichen Leistungsvereinbarung mit dem/der Auftraggeber:in wird der gesamte weitere Datensatz nach vorheriger Zustimmung des/der Auftraggeber:in datenschutzgerecht vernichtet. Auf Wunsch des/der Auftraggeber:in kann eine Kopie der Daten durch VisionGesund für den Fall einer Folgebeauftragung weiterhin digital archiviert werden.

3 Qualitätssicherung bei Befragungsprojekten

Äußere Form des Fragebogens (Online und Papier)

Bei der Erstellung des Fragebogens wird auf ein verständliches Layout Wert gelegt. Dies bezieht sowohl die Gestaltung bzw. Darstellung der Frage als auch die Anzahl der Fragen pro Seite mit ein. Bei Online-Befragungen kann der Fragebogen in Bezug auf die Barrierefreiheit für Screenreader-Lösungen optimiert werden, sofern von dem/der Auftraggeber:in gewünscht. Hier beträgt die maximale Anzahl zwei Fragen je Seite. Bei Papier- und Stiftbefragungen wird ebenfalls auf eine angemessene Zahl an Fragen pro Seite geachtet. Ferner wird ein hoher Kontrast in der Darstellung gewählt.

Pre-Test Fragebogen

Findet Anwendung, wenn ein individueller bzw. individuell modifizierter Fragebogen zusammengestellt wird.

Nach der Erstgestaltung des Fragebogens wird ein Pre-Test durchgeführt, um die Richtigkeit des Fragebogens zu testen und mögliche Verbesserungsvorschläge einzuarbeiten. Hierzu erhält der/die Auftraggeber:in einen Link, der ihn zur Online-Befragung weiterleitet, oder ihm wird, im Falle einer Papier- und Stiftbefragung, einen Testbogen zugesandt.

Beim Pre-Test hat der/die Auftraggeber:in die Möglichkeit, Anmerkungen zu jeder einzelnen Frage anzugeben. Ferner können Rückmeldungen zu der Schriftgröße, dem Farbschema oder dem Fragenlayout gegeben werden. Im Anschluss werden die Anmerkungen von VisionGesund eingearbeitet und der Fragebogen zur finalen Freigabe an den/die Auftraggeber:in gesendet.

Rücklaufkontrolle

In Bezug auf den Rücklauf der Befragung findet eine tägliche Kontrolle der aktuell abgeschlossenen Interviews statt. Nach Abschluss jeder Woche des Befragungszeitraums informiert VisionGesund den/die Auftraggeber:in über die aktuelle Rücklaufquote. Sollte die Rücklaufquote geringer als 50 %

ausfallen, so empfiehlt VisionGesund erneute Maßnahmen zur Steigerung der Teilnahme an der Befragung.

Information der Mitarbeiter:innen

Vorbereitende und begleitende Informationen an die Mitarbeiter:innen (d. h. Informationen zum Ziel der Befragung, Hinweise auf die Freiwilligkeit, Informationen zur Wahrung der Anonymität und des Datenschutzes, Benennung von Ansprechpartnern für Rückfragen oder bei technischen Schwierigkeiten) erfolgen durch den/die Auftraggeber:in. Hierbei steht VisionGesund unterstützend zur Seite.

Darüber hinaus kann sich VisionGesund im Rahmen der Auftaktveranstaltung für die Mitarbeitenden persönlich vorstellen. Dies ist vorab zu vereinbaren.

Support bei Befragungen

Vorab, während sowie im Nachgang der Befragung bietet VisionGesund den Teilnehmer:innen Hilfe und Unterstützung an. Auf diesen Support wird in Absprache zusätzlich zum Fragebogen auch in Informationsschreiben an die Mitarbeiter:innen hingewiesen.

Qualitätsprozess während E-Mail-Kontakt

Im Rahmen von Mitarbeitendenbefragungen richtet VisionGesund eine spezifische E-Mail-Adresse für die Befragung ein. Dadurch stellt VisionGesund sicher, dass ein:e Ansprechpartner:in genannt wird und zur Verfügung steht. Der Kontakt mit Teilnehmer:innen erfolgt über diese E-Mail-Adresse in folgenden Schritten:

Tabelle 2: Übersicht der einzelnen Prozessschritte bei E-Mail-Kontakt

Prozessschritt	Erklärung	Zugriffbeschränkung	Zeitraum
E-Mail-Versendung durch Teilnehmer:in	Teilnehmer:in nimmt Kontakt zu VisionGesund über die eingerichtete E-Mail-Adresse auf	Teilnehmer:in	Einmalig
Erhalt der E-Mail durch VisionGesund	Die E-Mail wird auf den VisionGesund Servern gespeichert	VisionGesund	Gesamte Dauer des Befragungszeitraums
Antwort per E-Mail durch VisionGesund	VisionGesund nimmt Kontakt zum/r Teilnehmer:in auf	VisionGesund	Innerhalb von 24 Stunden an Werktagen
Erneute Antwort durch Teilnehmer:in und VisionGesund	Gegebenenfalls werden wechselseitige Antworten erfolgen	Teilnehmer:in, VisionGesund	Innerhalb von 24 Stunden an Werktagen

4 Datenanalyse

Die erhobenen Rohdaten werden auf Vollständigkeit und Validität überprüft. Der Datensatz wird entsprechend der nachfolgenden Schritte um Ausreißer und Verzerrungspotentiale bereinigt.

Prüfung auf Vollständigkeit und Validität

Es ist möglich, dass Mitarbeiter:innen den Fragebogen nur teilweise beantworten bzw. Fragen mit einer Ausweichoption („keine Angabe“) beantworten. In diesem Fall erfolgt eine fallweise Bereinigung, wenn der Datensatz dadurch unvollständig wird. Datensätze werden als unvollständig eingestuft, sofern weniger als 50 % der Fragen beantwortet wurden oder wenn mehr als 50 % der Fragen mit der Ausweichoption („keine Angabe“) beantwortet wurden. Freiwillige Angaben werden bei diesem Orientierungswert nicht berücksichtigt.

Es ist ferner denkbar, dass Mitarbeiter:innen die Befragung nur oberflächlich durchklicken, ohne die Fragen zu lesen und entsprechend zu beantworten. Grundsätzlich werden deshalb alle Fälle mit doppelter Beantwortungsgeschwindigkeit – gemessen an der durchschnittlichen Beantwortungsdauer aller Fälle – von der Auswertung ausgeschlossen. In diesen Fällen ist anzunehmen, dass die Fragen nicht gelesen wurden.

Häufigkeitsverteilung (numerisch und prozentual)

Um einen ersten Aufschluss über die Ergebnisse der Online-Befragung zu bekommen, werden deskriptive Häufigkeitsverteilungen angeführt. Diese ermöglichen es, erste Trends der Teilnahme und Ergebnisse in Bezug auf relevante Faktoren (Standort, Abteilung, Tätigkeitsbereich u. a.) abzuleiten.

Berechnung der Mittelwerte inklusive Standardabweichung

Ziel der Datenauswertung ist es unter anderem, Unterschiede in den Skalen und Items festzustellen. Hierzu wird zunächst das arithmetische Mittel zu allen Skalen und Items berechnet sowie die jeweilige Standardabweichung überprüft.

Mittelwertvergleich

Im nächsten Schritt wird geprüft, ob es statistisch signifikante Unterschiede zwischen den Mittelwerten bei unterschiedlich großen Gruppen gibt. Hierzu wird je nach Befragungstyp ein One-Way ANOVA Test mit Tukey Kramer Post Hoc Test durchgeführt.

Die folgende Tabelle fasst die möglichen statistischen Tests übersichtlich zusammen:

Tabelle 3: Statistische Test bei Befragungsprojekten

Auswertungsschritt	Erklärung
Prüfung auf Ausfüllgeschwindigkeit	Prüfung, ob die Geschwindigkeit des Ausfüllens schneller oder langsamer als der Durchschnitt ist (Ausreißer bereinigt): Ausschluss ab 2,1-facher Ausfüllgeschwindigkeit oder Ausreißern auf den inhaltsbezogenen Seiten der Befragungen. Gegebenenfalls fallweiser Ausschluss.
Häufigkeitsverteilung (absolut und prozentual)	Deskriptive Analysen der Trends der Teilnahme und Ergebnisse in Bezug auf relevante Faktoren (Tätigkeitsbereich, Geschlecht, Altersgruppe u. a.).

Mittelwertvergleich	Mittelwertvergleiche für Gruppen mit unterschiedlichen Größen geben Aufschluss, ob statistisch signifikante Unterschiede zwischen relevanten Gruppen (Tätigkeitsbereich, Führungsaufgabe, u. a.) vorliegen.
Anzahl Teilnehmer:innen	Die Anzahl der berücksichtigten Antworten werden zu allen Skalen und Items ausgewiesen. Ausweichoptionen (z. B. „Keine Angabe“) werden nicht berücksichtigt.
Mittelwerte	Das arithmetische Mittel wird zu allen Skalen und Items berechnet, zu denen mindestens die definierte Anzahl an Antworten zur Auswertung eingegangen ist.
Standardabweichung	Die Standardabweichung wird zu allen Skalen und Items berechnet, zu denen mindestens die definierte Anzahl an Antworten zur Auswertung eingegangen ist.

5 Datenanalyse bei Screening-Verfahren/Grobanalyse

Für Screening-Verfahren/Grobanalysen gilt ein in Teilen abweichendes Vorgehen gegenüber den Ausführungen in Kapitel 1.*4 Datenanalyse*. Ziel eines Screening-Verfahrens/der Grobanalyse ist die Identifikation belastender Faktoren (Fragen) in einzelnen Gruppen (z. B. Analysebereiche). Ursachen hierzu werden regelmäßig im anschließenden Follow-Up Prozess, bestehend aus einem Workshop zur Feinanalyse und einem Workshop zu Maßnahmenplanung, herausgearbeitet.

Prüfung auf Vollständigkeit und Validität

Vollständigkeit und Validität werden entsprechend den Ausführungen im vorangegangenen Kapitel überprüft (*Kapitel 1.4 Datenanalyse*).

Häufigkeitsverteilung (numerisch und prozentual)

Im Screening werden – je nach Auftrag – absolute und relative Teilnahmedaten einzelner Tätigkeitsbereiche erhoben. Soziodemographische Daten werden nicht regelmäßig erhoben, wodurch keine diesbezüglichen Häufigkeitsverteilungen ermittelt werden. Ausnahmen werden explizit mit dem/der Auftraggeber:in abgestimmt. Zusätzlich wird die Anzahl der beantworteten Fragen insgesamt bzw. die Anzahl der ausgewählten Ausweichoptionen im Fragebogen („keine Angabe“) bezogen auf die einzelnen Fragen ermittelt und ausgewiesen. Entsteht hierdurch ein verwertbare Antwortzahl von n<5 wird die Frage nicht weiter ausgewertet.

Berechnung der Mittelwerte inklusive Standardabweichung

Im Screening-Verfahren/der Grobanalyse sollen besonders belastende Faktoren (Fragen) herausgearbeitet werden. Zu diesem Zweck werden die Antwortmöglichkeiten mit Punktwerten versehen (z. B. „Nein, gar nicht“=1 Punkt, „Ja, genau“=5 Punkte). Aus diesen Punktwerten wird ein Mittelwert errechnet. Regelmäßig gilt: Je höher der Wert, desto besser wurde die Frage insgesamt beantwortet und desto geringer erscheint die daraus resultierende Belastung insgesamt in der betrachteten Population. Invertierte Fragen, also Fragen mit umgekehrter Antwortskale, werden bei der Berechnung des Mittelwerts entsprechend berücksichtigt. Die errechneten Mittelwerte dienen

dem Vergleich der Fragen zueinander und der Identifikation von Belastungsschwerpunkten, die als Grundlage für den Follow-Up Prozess dienen.

6 FAQ

Welche Daten werden erhoben?

Es werden ausschließlich Daten erhoben, die der inhaltlichen Auswertung der Umfrage dienen.

Können Eingaben zurückverfolgt werden?

Nein. Es werden keine Daten erhoben – weder inhaltlich noch formal –, die Rückschlüsse auf einzelne Personen zulassen.

Wie wird die Anonymität technisch gesichert?

Es werden keine IP-Adresse gespeichert. So bleiben alle Daten auch technisch anonym. Zudem wir nur ein einziger Cookie gespeichert, der sogenannte Session-Cookie. Dieser gewährleistet, dass die bearbeitenden Person aus der Befragung ausgeloggt wird, sobald die Personen den eigenen Browser schließt. Damit stärkt dieser Cookie den Datenschutz.

Auf welchen Servern werden die Daten erhoben?

Die Daten werden auf den virtuellen Servern der VisionGesund GmbH erhoben. Betreiber des Servers ist die Microsoft Corporation.

Wem gehören die Server?

Die Server werden im Rechenzentrum der Microsoft Corporation betrieben.

Wo stehen die Server?

Die Server stehen in der Europäischen Union.

Wer betreibt die Server?

Der technische Betrieb wird von die InterNetWire Communications GmbH durchgeführt.

Wer hat Zugriff auf die Daten?

Ausschließlich die VisionGesund GmbH (nur projektverantwortliche Mitarbeiter:innen).

In welcher Form werden die Daten gespeichert?

Der Rohdatensatz der Umfrageergebnisse wird temporär und ausschließlich zur Auswertung auf dem lokalen Datenträger der VisionGesund GmbH gespeichert. Die Auswertung erfolgt über eine Vision-Gesund eigene Software-Lösung, welche die Serverstrukturen von Microsoft Azure nutzt. Die Auswertungsergebnisse werden hier temporär und ausschließlich zur Berichterstellung gespeichert. Die Ergebnisse werden anschließend auf den VisionGesund eigenen Servern gespeichert, bis sie dem/der Kund:in übergeben werden. Unter Rücksprache mit dem/der Auftraggeber:in können digitale Kopien von Ergebnisberichten archi-viert werden.

Wie lange werden die Daten gespeichert?

Im Rahmen der Beratungsverträge ist geregelt, dass der bereinigte Rohdatensatz automatisch in pseudonymisierter Form in die Benchmark-Datenbank von VisionGesund als pseudonymisierter Datensatz integriert werden. Über einen automatisch generierten Hash-Wert kann der pseudonymisierte Datensatz für den sogenannten historischen Benchmark entschlüsselt und nutzbar gemacht werden.

Mit Beendigung des Beratungsvertrags werden die Projektdaten aus dem Befragungssystem – mit Ausnahme der o.g. Benchmark-Datenbank – gelöscht. D.h. der gespeicherte Rohdatensatz wird nach abgeschlossenem Projektzeitraum von der Projektleitung vom Datenträger der VisionGesund GmbH vollständig gelöscht, ebenso erfolgt eine Löschung des Datensatzes in Azure nach Projektende. Die Löschung von Ergebnisberichten erfolgt in Abstimmung mit dem Auftraggeberin.

Wer ist für die Datenvernichtung verantwortlich?

Wird die Löschung von Datensätzen im Beratungsvertrag vereinbart, so wird die Löschung der Datensätze inkl. Dokumentation durch die VisionGesund GmbH durchgeführt.

Technisch-organisatorische Maßnahmen

Hinweis: Anlage 1 bezieht sich auf die Datenverarbeitung des Dokumentenmanagementsystems der VisionGesund GmbH. Die technisch und organisatorischen Maßnahmen der Befragungsplattform VisionInsight wird in Anlage 4 gesondert spezifiziert.

Gemäß § 5 der Vereinbarung zur Auftragsverarbeitung verweist die AV zur Konkretisierung der technisch organisatorischen Maßnahmen auf diesen Anhang.

(1) Technische und organisatorische Sicherheitsmaßnahmen: Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.
(2) Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters: Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.
(3) Konkretisierung der Einzelmaßnahmen: Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahmen
1.	**Zutrittskontrolle** Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Folgende Strukturen werden angewendet: • Physische Zugangskontrolle: Installation von Schließanlagen, um den Zugang zu Gebäuden zu kontrollieren (Schlüsselregelung, Schlüsselausgabe etc.) • Elektronisches Zutrittssystem/Schließanlage • Erstellung, Zuordnung und Verwendung von Mitarbeiter:innenprofilen • Multi-Faktor-Authentifikation von Mitarbeiter:innen • Sorgfältige Auswahl von Mitarbeiter:innen • Sorgfältige Auswahl von Reinigungspersonal • Schulung der Mitarbeiter über Sicherheitsrichtlinien, Verfahren zur Zutrittskontrolle und die Bedeutung der Einhaltung von Sicherheitsmaßnahmen, um das Bewusstsein für Sicherheitsrisiken zu erhöhen
2.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von	Folgende Strukturen werden angewendet: • Erstellung, Zuordnung und Verwendung von Mitarbeiter:innenprofilen

	Unbefugten genutzt werden können.	• Multi-Faktor-Authentifikation von Mitarbeiter:innen • Verbindlicher Passwort-Kodex. Einsatz und Kontrolle einer strengen Passwortvergabe • Schlüsselregelung (Schlüsselausgabe etc.) • Zuordnung von Mitarbeiter:innenprofilen zu IT-Systemen • Einsatz sicherer Netzwerkprotokolle (wie HTTPS) • Automatische Bildschirmsperre • Anwendungsbezogener Login • Einsatz von Anti-Viren-Software • Managed UTM Firewall
3.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Folgende Strukturen werden angewendet: • Mitarbeiter:innen-Identifikation und Authentifizierung: • Die vom Auftragnehmer genutzten Systeme bieten verschiedene Authentifizierungsmethoden an, wie beispielsweise Multi-Faktor-Authentifizierung (MFA), um sicherzustellen, dass nur berechtigte Mitarbeiter:innen auf die Systeme zugreifen können. Berechtigungen: • Der Auftragnehmer vergibt verschiedene Berechtigungsstufen und -rollen für Mitarbeiter:innen und Gruppen, um sicherzustellen, dass sie nur auf die Daten zugreifen können, für die sie autorisiert sind. Audit-Protokolle: • Die vom Auftragnehmer genutzten Systeme bieten Audit-Protokolle an, um Mitarbeiter:innen-Aktivitäten und -zugriffe nachvollziehen zu können. Verschlüsselung: • Die vom Auftragnehmer genutzten Systeme bieten Funktionen zur Datenverschlüsselung sowohl während

		der Übertragung als auch beim Speichern von Daten. Sichere Netzwerkprotokolle: • Für den sicheren Zugriff von externen Standorten werden sichere Netzwerkprotokolle (wie HTTPS) genutzt werden. Automatisierte Kontrollen: • Die vom Auftragnehmer genutzten Systeme ermöglichen es, Policies und Regeln zu definieren, um ungewöhnliche Zugriffe automatisch zu erkennen und entsprechende Maßnahmen zu ergreifen, etwa Benachrichtigungen oder das temporäre Sperren von Konten. Schulungen: • Schulungen der Mitarbeiter:innen des Auftragnehmers mit datenschutzrelevanten Daten und die Sensibilisierung für mögliche Risiken sind ebenfalls ein wichtiger Bestandteil der Zugangskontrolle. Schutz vor kriminellem Zugriff: • Einsatz einer Cyber-Privacy-Protection-Software zum Schutz der Online- und Offline-Privatsphäre
4.	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur	Folgende Strukturen werden angewendet: • Einsatz sicherer Netzwerkprotokolle (wie HTTPS) • Digitale Signatur in der elektronischen Kommunikation • Revisionssichere Archivierung der E-Mails • Protokollierung und Überwachung von Datenweitergaben an Dritte, um eine Nachverfolgbarkeit und Transparenz sicherzustellen • Schulung der Mitarbeiter:innen über sichere Kommunikationswege

	Datenübertragung vorgesehen ist.	
5.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Folgende Strukturen werden angewendet: • Authentifizierung: Implementierung von Mechanismen zur Identifizierung und Überprüfung von Mitarbeiter:innen, um sicherzustellen, dass nur autorisierte Personen auf das System oder die Anwendung zugreifen können • Verwendung von Passwörtern, biometrischen Merkmalen, Zwei-Faktor-Authentifizierung • Kontrolle und Beschränkung der Zugriffsberechtigungen von Mitarbeiter:innen auf bestimmte Daten oder Funktionen basierend auf ihren jeweiligen Rollen und Verantwortlichkeiten • Einsatz von Verschlüsselungstechnologien, um sensible oder vertrauliche Eingaben während der Übertragung zu schützen • Nachverfolgbarkeit von Eingabe und Änderungen • Schulung der Mitarbeiter:innen über sichere Eingabepraktiken und die Bedeutung der Einhaltung von Sicherheitsrichtlinien, um das Risiko von Sicherheitsvorfällen oder Datenschutzverletzungen zu minimieren
6.	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	Folgende Strukturen werden angewendet: • Unterauftragsverarbeitungskontrolle: Abschluss von Verträgen oder Vereinbarungen mit Subunternehmern, um sicherzustellen, dass auch Unterauftragsverarbeiter die erforderlichen Datenschutzstandards einhalten • Festlegung klarer Verfahren zur Meldung von Datenschutzverletzungen an die Verantwortlichen • Abschluss von schriftlichen Datenschutzvereinbarungen mit Mitarbeiter:innen • Durchführung von Einweisungen und Schulungen der Mitarbeiter:innen
7.	**Verfügbarkeitskontrolle**	Folgende Strukturen werden angewendet:

	Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	• Cyber-Privacy-Protection-Software zum Schutz der Online- und Offline-Privatsphäre • Systematische und regelmäßige Backups • Geografische Redundanz: Verteilung von Daten und Diensten über mehrere geografische Standorte • Durchführung regelmäßiger Wartungsarbeiten, Updates und Patch-Management, um die Sicherheit und Stabilität von Systemen und Anwendungen zu gewährleisten und potenzielle Sicherheitslücken zu schließen • Rechtskonforme Archivierung/ Sicherung von relevanten, projektbezogenen Inhalten (DSGVO /GoBD)
8.	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Folgende Strukturen werden angewendet: • Festlegung definierter Rollen und entsprechender Zugriffsrechte für Mitarbeiter:innen basierend auf ihren jeweiligen Aufgaben und Verantwortlichkeiten • Unterteilung des Dokumentenmanagements in Segmente mit unterschiedlichen Zugriffsebenen. Dadurch werden sensible Daten von weniger sensiblen Daten getrennt und der Zugriff entsprechend eingeschränkt • Durchführung von Einweisungen und Schulungen von der Mitarbeiter:innen • Stichprobenkontrollen, um den Zugriff auf Daten zu protokollieren und zu überwachen

(4) Die Konsistenz der Technisch-organisatorische Maßnahmen wird regelmäßig überprüft, bewertet und gegebenenfalls Verbesserungsmaßnahmen eingeleitet. Hierzu verpflichtet sich der Auftragnehmer, eigenverantwortlich interne Audits durchzuführen.

Spezifika der von VisionGesund bereitgestellten Befragungsplattform VisionInsight

Für die technische Umsetzung werden die folgenden Aspekte berücksichtigt. Diese betreffen den Schutz der Daten, die Einhaltung rechtlicher Vorgaben und die Bereitstellung von Mechanismen zur Wahrung der Betroffenenrechte:

Verschlüsselung

Transportverschlüsselung (TLS): Alle Datenübertragungen zwischen Nutzer und Plattform sind durch HTTPS gesichert. Vermeidung von unsicheren Protokollen wie HTTP oder unverschlüsseltem FTP.

Speicherverschlüsselung & Passwortsicherheit: Sensible Daten, wie Passwörter werden verschlüsselt in der Datenbank gespeichert werden. Hierzu werden von Algorithmen wie AES-256 für gespeicherte Daten eingesetzt. Die Speicherung von Passwörtern erfolgt als Hash im Standard HMACSHA512.

Zugriffskontrolle

Benutzer-Authentifizierung: Einsatz von sicheren Passwortrichtlinien (Mindestlänge, Komplexität).

Zugriffsberechtigungen: Vergabe eines rollenbasierten Zugriffssystems (Role-Based Access Control, RBAC). Zugriff auf sensible Daten nur für autorisierte Nutzer:innen.

Datenminimierung und -speicherung

Erhebung minimaler Daten: Es werden ausschließlich Daten erfasst, die für den Betrieb der Plattform notwendig sind.

Backup-Verwaltung: Verschlüsselte Speicherung von Backups und deren Löschung nach Ablauf der Speicherfrist.

Sicherheit der IT-Infrastruktur

Sicherheitsupdates: Regelmäßige Aktualisierung der Software und Betriebssysteme, um Sicherheitslücken zu schließen via Patchmanagement.

DDoS-Schutz: Maßnahmen zur Erkennung und Blockierung von automatisierten Angriffen in Echtzeit, um die Erreichbarkeit und Sicherheit der gehosteten Dienste zu gewährleisten.

Protokollierung und Monitoring

Log-Dateien: Erfassung von Systemereignissen (Login-Versuche, Datenzugriffe) mit beschränktem Zugriff.

Einhaltung der Betroffenenrechte

Auskunft und Datenexport: Nutzer:innen können jederzeit Auskunft über Ihre Daten einfordern oder alle personenbezogenen Daten löschen lassen.

Cookies und Tracking

Cookie-Management: Cookies werden grundsätzlich nicht erhoben. Die einzige Ausnahme ist der sogenannte Session-Cookie. Dieser gewährleistet, dass die bearbeitenden Person aus der Befragung

ausgeloggt wird, sobald die Personen den eigenen Browser schließt. Damit stärkt dieser Cookie den Datenschutz.

IP-Anonymisierung: IP-Adressen werden nicht erfasst.

Subunternehmer und Dritte

Integration externer Dienste: Verträge zur Auftragsverarbeitung mit Drittanbietern (siehe Anlage 2).

Sicherstellung der DSGVO-Konformität: Überprüfung der Datenschutzmaßnahmen der Dienstleister.

Schutz vor Datenverlust

Datensicherung: Regelmäßige Erstellung von Backups, die verschlüsselt und getrennt gespeichert werden. 30 Tage rückwärts gibt es ein tägliches Backup der Datenbanken.

Notfallpläne: Maßnahmen zur schnellen Wiederherstellung der Daten und Systeme im Fall von Cyberangriffen oder technischen Ausfällen.