Hochschule Karlsruhe
University of
Applied Sciences

Datenschutz-Folgenabschätzung

für die Gesundheitsapp „Mein ias“

16. Juni 2025

Max Mustermann	Matrikel-Nr.: 123456
Erika Musterfrau	Matrikel-Nr.: 234567
John Doe	Matrikel-Nr.: 345678
Jan-David Wiederstein	Matrikel-Nr.: 825713

Hochschule Karlsruhe
Data Science B.Sc.
Modul: Datenschutz / Ethik
Dozent: Prof. Dr. Datenschutz

Inhaltsverzeichnis

1 Einleitung und Rahmenbedingungen

Die geplante Einführung der Gesundheitsapp „Mein ias“ der ias AG für ca. 1500 Mitarbeitende von Unternehmen XY beinhaltet datenschutzrechtliche Risiken, insbesondere wegen der Verarbeitung sensibler Gesundheitsdaten (Art. 9 DSGVO) im Rahmen freiwilliger Checks und eines potenziellen Interessenkonflikts, da ias-Personal sowohl Gesundheitsmanagement (App) als auch Arbeitssicherheitsaufgaben wahrnimmt.

Die Nutzung erfolgt vollständig freiwillig, sowohl hinsichtlich der Registrierung als auch der Gesundheitsangebote. Damit ist die Voraussetzung für eine wirksame Einwilligung gemäß Art. 9 Abs. 2 lit. a DSGVO grundsätzlich erfüllt. Dennoch muss die Freiwilligkeit durch geeignete Maßnahmen abgesichert werden (z.B. keine Nachteile bei Nichtteilnahme, keine arbeitsrechtliche Bewertung).

Weiterhin kritisch ist die Doppelrolle der ias AG sowie die Frage, ob Gesundheitsdaten hinreichend geschützt und anonymisiert verarbeitet werden.

Wichtigste Maßnahmen: Einholung wirksamer, ausdrücklicher Einwilligungen (Art. 9 Abs. 2 lit. a DSGVO, § 26 Abs. 2 BDSG), Abschluss eines konformen Auftragsverarbeitungsvertrags (AVV) mit Prüfung der Technisch-Organisatorischen Maßnahmen (TOMs) der ias AG (v. a. Zugriffskontrolle, Anonymisierung), Minimierung des Interessenkonflikts durch technische/organisatorische Trennung (ideal: personelle Trennung der Rollen). Eine Datenschutz-Folgenabschätzung (DSFA) bleibt nach Art. 35 DSGVO weiterhin notwendig.

Fazit: Die App kann unter Bedingungen datenschutzkonform eingesetzt werden. Die Freiwilligkeit reduziert zentrale Risiken, der Interessenkonflikt und die technische Umsetzung erfordern dennoch strenge Kontrollmaßnahmen. Eine vorherige Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) wird empfohlen.

2 Beschreibung der Verarbeitungsvorgänge

2.1 Allgemeine Projektbeschreibung

Der Arbeitgeber bietet seinen Mitarbeitern die freiwillige Nutzung der Gesundheitsapp „Mein ias“ an. Die App dient als Plattform für Gesundheitsinformationen und ermöglicht die Durchführung von Gesundheitschecks mittels Fragebögen.

Onboarding-Prozess: Die Registrierung und Nutzung der App sind für alle Mitarbeiter vollständig freiwillig. Entscheidet sich ein Mitarbeiter zur Teilnahme, ist die Angabe der Firmen-E-Mail-Adresse für die Registrierung verpflichtend. Laut Anbieter dient dies der reinen Zuordnung zum Unternehmen und der Verifizierung der Nutzungsberechtigung.

Einwilligungen: Notwendige Einwilligungen, insbesondere zur Verarbeitung von Gesundheitsdaten, werden im Registrierungsvorgang vom jeweiligen Mitarbeiter eingeholt.

Freiwilligkeit: Da die Teilnahme von Anfang an freiwillig ist, ist die Freiwilligkeit der Einwilligung (Art. 7 DSGVO) grundsätzlich gegeben.

Rollenverteilung nach DSGVO: Der Arbeitgeber ist Verantwortlicher (Art. 4 Nr. 7 DSGVO), die ias AG Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO). Die gegenteilige Auffassung der

ias AG ist nicht haltbar. Ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO ist zwingend erforderlich.

2.2 Zwecke der Verarbeitung

- Verwaltung der Nutzerkonten und Authentifizierung.
- Durchführung von Gesundheitschecks auf freiwilliger Basis.
- Bereitstellung von Gesundheitsinformationen.
- Unterstützung präventiver Gesundheitsmaßnahmen des Arbeitgebers.
- Erstellung anonymisierter Statistiken für den Arbeitgeber.

2.3 Rechtsgrundlagen der Verarbeitung

- **Registrierung (Firmen-E-Mail):** Die Verarbeitung stützt sich auf die Einwilligung des Nutzers durch den freiwilligen Registrierungsakt (Art. 6 Abs. 1 lit. a DSGVO) sowie auf das berechtigte Interesse des Arbeitgebers (Art. 6 Abs. 1 lit. f DSGVO), die Nutzung auf betriebszugehörige Mitarbeiter zu beschränken.
- **Gesundheitsdaten:** Die Verarbeitung stützt sich ausschließlich auf die ausdrückliche Einwilligung der Mitarbeiter (Art. 9 Abs. 2 lit. a DSGVO).

2.4 Verarbeitete Datenkategorien

- **Kontaktdaten:** Dienstliche E-Mail-Adresse.
- **Gesundheitsdaten (Art. 4 Nr. 15 DSGVO):** Antworten aus den freiwillig ausgefüllten Fragebögen.
- **Nutzungs- und Gerätedaten:** Potenziell IP-Adresse, Gerätekennungen, Login-Zeiten. Dies muss mit dem Anbieter geklärt werden.

2.5 Betroffene Personen

Kreis der betroffenen Personen sind die Mitarbeiter des Unternehmens, die sich freiwillig entscheiden, die App zu nutzen.

2.6 Verarbeitungsmittel und Technologien

Die Verarbeitung erfolgt primär über die mobile App „Mein ias“, die auf einer von der ias AG betriebenen Server-Plattform läuft. Folgende Technologien sind relevant:

- **Anonymisierungs-/Pseudonymisierungsverfahren:** Es ist geplant, dass die für Statistiken verwendeten Daten anonymisiert werden. *[Anmerkung: Die genaue technische Methode der Anonymisierung (z.B. k-Anonymität, l-Diversität) muss von der ias AG offengelegt und auf ihre Wirksamkeit geprüft werden, um eine Re-Identifizierung auszuschließen.]*
- **Verschlüsselung:** Datenübertragungen zwischen App und Server sollten mittels aktueller Transportverschlüsselung (z.B. TLS 1.3) geschützt sein. Datenbanken sollten

verschlüsselt sein (Encryption-at-rest). *[Anmerkung: Die spezifischen Verschlüsselungsalgorithmen und die Schlüssellängen sind zu verifizieren.]*

- **Tracking/Profiling-Technologien:** Es ist zu klären, ob über die reine Funktionsbereitstellung hinaus Tracking-Technologien (z.B. für Nutzungsanalysen) oder Profiling-Algorithmen (z.B. für die Erstellung von Risikoprofilen) eingesetzt werden. *[Anmerkung: Eine vollständige Offenlegung etwaiger Tracking- oder Profiling-Mechanismen durch die ias AG ist für eine abschließende Bewertung unerlässlich.]*

2.7 Empfänger der Daten

- **Die ias Aktiengesellschaft:** Als Auftragsverarbeiter primärer Empfänger aller Datenkategorien.
- **Mögliche Unterauftragsverarbeiter:** Dienstleister der ias AG (z.B. für Hosting). Diese müssen offengelegt und vom Arbeitgeber genehmigt werden.
- **Interne Stellen beim Arbeitgeber:** Empfänger ausschließlich der anonymisierten Statistiken.

2.8 Datenflüsse

- **Eingabe:** Mitarbeiter gibt seine E-Mail-Adresse bei der Registrierung sowie Antworten in den Gesundheitsfragebögen in die App ein.
- **Übertragung:** Die Daten werden verschlüsselt von der App an die Server-Infrastruktur der ias AG übertragen.
- **Verarbeitung & Speicherung:** Die ias AG speichert die Daten und verarbeitet sie zur Bereitstellung der App-Funktionen.
- **Anonymisierung & Aggregation:** Für die Statistik-Erstellung werden Gesundheitsdaten aus den Fragebögen anonymisiert und aggregiert.
- **Bereitstellung Statistik:** Die anonymisierte Statistik wird dem Arbeitgeber (z.B. Personalabteilung) zur Verfügung gestellt.
- **Löschung:** Bei Widerruf der Einwilligung oder nach Beendigung des Nutzungsverhältnisses werden die personenbezogenen Daten des Mitarbeiters gelöscht.

2.9 Speicherdauer und Löschkonzept

Gemäß dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) dürfen Daten nur so lange gespeichert werden, wie es für den Zweck erforderlich ist.

- **Nutzerkonten und Stammdaten:** Löschung unverzüglich nach Widerruf der Einwilligung oder Beendigung der App-Nutzung durch den Mitarbeiter.
- **Gesundheitsdaten:** Löschung ebenfalls unverzüglich nach Widerruf der spezifischen Einwilligung für die Gesundheitschecks.
- **Backups:** Definition von Aufbewahrungsfristen für Backups und Sicherstellung, dass Löschanträge auch dort umgesetzt werden (innerhalb einer angemessenen Frist).

[Anmerkung: Ein detailliertes Löschkonzept fehlt bislang und muss von der ias AG zwingend vorgelegt werden. Dieses muss die genauen Fristen und die technischen Prozesse zur sicheren Löschung (nicht nur Deaktivierung) der Daten beschreiben.]

2.10 Internationale Datenübermittlung

Es wird davon ausgegangen, dass die Verarbeitung ausschließlich in der EU/dem EWR stattfindet. *[Anmerkung: Der Arbeitgeber muss sich von der ias AG schriftlich bestätigen lassen, dass alle Daten (inkl. Backups) und alle eingesetzten Unterauftragsverarbeiter ihren Sitz und ihre Verarbeitungsstandorte ausschließlich innerhalb der EU/des EWR haben. Sollte ein Drittlandtransfer stattfinden, wäre eine separate, detaillierte Prüfung der Rechtsgrundlage (z.B. Angemessenheitsbeschluss, Standardvertragsklauseln nach Art. 46 DSGVO inkl. Transfer Impact Assessment) zwingend erforderlich.]*

2.11 Beschreibung der (geplanten) Technischen und Organisatorischen Maßnahmen (TOMs)

Die ias AG als Auftragsverarbeiter muss gemäß Art. 32 DSGVO geeignete TOMs nachweisen, um die Sicherheit der Daten zu gewährleisten. Zu prüfen sind insbesondere:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme.
- Zugriffs-, Zugangs- und Zutrittskontrollkonzepte: Wer darf auf welche Daten wie zugreifen?
- Trennungskontrolle: Mandantenfähigkeit der Systeme, um Daten verschiedener Kunden sauber zu trennen.
- Prozesse zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs.
- Incident-Response-Management: Prozesse zur Erkennung und Meldung von Datenschutzverletzungen.

[Anmerkung: Eine vollständige Dokumentation der von der ias AG implementierten TOMs nach Art. 32 DSGVO liegt noch nicht vor. Diese ist im Rahmen des Abschlusses des Auftragsverarbeitungsvertrags anzufordern und auf Angemessenheit zu prüfen.]

3 Notwendigkeit und Verhältnismäßigkeit

3.1 Notwendigkeit der Verarbeitung für die Zwecke

Der Arbeitgeber verfolgt legitime Zwecke der Gesundheitsförderung. Die Nutzung einer App ist hierfür ein modernes und geeignetes, wenn auch nicht das einzige Mittel. Da die Nutzung freiwillig ist, ist die Verarbeitung der Daten der teilnehmenden Mitarbeiter notwendig, um ihnen den gewünschten Dienst überhaupt zur Verfügung stellen zu können. Die Verarbeitung ist somit auf den Kreis derjenigen beschränkt, die sie selbst anstoßen.

3.2 Angemessenheit und Erforderlichkeit der Daten (Datenminimierung)

Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) wird durch das neue Modell deutlich besser beachtet.

- **Firmen-E-Mail-Adresse:** Es werden nur noch die E-Mail-Adressen der Mitarbeiter verarbeitet, die sich aktiv registrieren. Die Vorgabe, die Firmen-E-Mail zu nutzen, ist zur Verifizierung der Berechtigung erforderlich und somit im Einklang mit dem Grundsatz der Datenminimierung.
- **Inhalte der Gesundheitsfragebögen:** Hier bleibt die Anforderung bestehen, dass nur Daten erhoben werden dürfen, die für den jeweiligen Zweck des Checks unbedingt erforderlich sind.

3.3 Verhältnismäßigkeit im Beschäftigungskontext

Die Abwägung zwischen den Interessen des Arbeitgebers und den Rechten der Beschäftigten fällt nun anders aus.

- **Interessen des Arbeitgebers:** Förderung der Gesundheit, Steigerung der Arbeitgeberattraktivität.
- **Rechte und Interessen der Mitarbeiter:** Schutz sensibler Gesundheitsdaten.

Da die gesamte Verarbeitung auf einer freien Entscheidung des Mitarbeiters beruht, ist der Eingriff in das Recht auf informationelle Selbstbestimmung durch den Mitarbeiter selbst legitimiert. Das entscheidende Risiko einer unzulässigen Druckausübung oder eines Zwangs entfällt. Die Maßnahme ist somit in ihrer Grundkonzeption verhältnismäßig.

Die verbleibenden Risiken liegen in der Ausgestaltung:

- **Informeller Druck:** Der Arbeitgeber muss durch klare Kommunikation sicherstellen, dass keine Nachteile aus einer Nichtteilnahme entstehen.
- **Transparenz:** Die Einwilligungserklärungen müssen exzellent formuliert sein, um eine informierte Entscheidung zu gewährleisten.
- **Datensicherheit:** Die technischen und organisatorischen Maßnahmen der ias AG zum Schutz der Daten müssen streng geprüft werden.

Fazit zur Verhältnismäßigkeit: Der Eingriff ist durch die Freiwilligkeit gerechtfertigt und verhältnismäßig. Die Verantwortung verlagert sich hin zur Sicherstellung einer informierten Einwilligung und zur Gewährleistung der Datensicherheit beim Auftragsverarbeiter.

4 Risikoanalyse für die Rechte und Freiheiten der Betroffenen

4.1 Methodik der Risikobewertung

Die Risikobewertung erfolgt gemäß Art. 35 DSGVO durch die Identifizierung potenzieller Bedrohungen für die Rechte und Freiheiten der betroffenen Mitarbeiter. Jedes Risiko wird

anhand der geschätzten **Eintrittswahrscheinlichkeit** und der **Schwere des potenziellen Schadens** bewertet. Der Schaden bezieht sich auf mögliche physische, materielle oder immaterielle Nachteile wie Diskriminierung, Rufschädigung, finanzieller Verlust oder Verlust der Kontrolle über die eigenen Daten.

Die Risikostufen werden wie folgt klassifiziert:

- **Niedrig:** Geringe Wahrscheinlichkeit und geringer Schaden.
- **Mittel:** Kombinationen aus gering/mittel/hoch, die keine hohe Einstufung erfordern.
- **Hoch:** Hohe Wahrscheinlichkeit und/oder hohe Schadensschwere.
- **Sehr hoch:** Hohe Wahrscheinlichkeit und hohe bis sehr hohe Schadensschwere.

4.2 Identifizierte Risiken

4.2.1 Risiken bezüglich Rechtmäßigkeit und Legitimation

Risiko: Die Einwilligung der Mitarbeiter ist aufgrund von informellem Druck im Arbeitsverhältnis (Angst vor Nachteilen bei Nicht-Teilnahme) nicht wirklich freiwillig.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Hoch (Die primäre Rechtsgrundlage nach Art. 9 DSGVO wäre unwirksam, was die gesamte Verarbeitung illegal macht.)
- **Risikostufe: Hoch**

Risiko: Die Einwilligung ist nicht ausreichend informiert, da die Datenschutzerklärung oder die Informationen in der App unvollständig oder unverständlich sind.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Hoch (Eine nicht informierte Einwilligung ist ungültig.)
- **Risikostufe: Hoch**

4.2.2 Risiken bezüglich Zweckbindung, Datenqualität und Speicherbegrenzung

Risiko: Die Anonymisierung der für Statistiken genutzten Daten ist technisch unzureichend, sodass Rückschlüsse auf Einzelpersonen möglich sind (Re-Identifizierung).

- *Eintrittswahrscheinlichkeit:* Mittel (Effektive Anonymisierung ist technisch anspruchsvoll.)
- *Schwere des Schadens:* Sehr hoch (Der Arbeitgeber erhielte faktisch sensible Gesundheitsdaten einzelner Mitarbeiter, was zu Diskriminierung führen kann.)
- **Risikostufe: Sehr hoch**

Risiko: Daten werden aufgrund eines fehlenden oder nicht funktionierenden Löschkonzepts länger als notwendig gespeichert.

- *Eintrittswahrscheinlichkeit:* Hoch

- *Schwere des Schadens:* Mittel (Verstoß gegen Art. 5 Abs. 1 lit. e DSGVO, erhöht die Angriffsfläche bei Datenlecks.)
- **Risikostufe: Hoch**

4.2.3 Risiken bezüglich Transparenz

Risiko: Die Informationspflichten nach Art. 13 DSGVO werden unvollständig erfüllt (z.B. fehlende Angaben zu Unterauftragsverarbeitern oder zur genauen Logik der Statistik-Erstellung).

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Mittel (Mitarbeiter können keine fundierte Entscheidung treffen und ihre Rechte nicht wirksam wahrnehmen.)
- **Risikostufe: Mittel**

4.2.4 Risiken bezüglich Betroffenenrechte

Risiko: Anfragen auf Auskunft, Berichtigung oder Löschung können von der ias AG oder dem Arbeitgeber nicht fristgerecht oder nicht vollständig bearbeitet werden, weil die Prozesse dafür fehlen.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Mittel (Verstoß gegen Kapitel III DSGVO, führt zu Frustration und Kontrollverlust bei den Betroffenen.)
- **Risikostufe: Mittel**

4.2.5 Risiken bezüglich Datensicherheit

Risiko: Unbefugter externer (Hacker) oder interner (Mitarbeiter der ias AG) Zugriff auf die Datenbank mit Gesundheitsdaten.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Sehr hoch (Offenlegung hochsensibler Daten, Identitätsdiebstahl, Erpressung, soziale Stigmatisierung.)
- **Risikostufe: Sehr hoch**

4.2.6 Risiken bezüglich Auftragsverarbeitung

Risiko: Der Auftragsverarbeitungsvertrag (AVV) zwischen dem Arbeitgeber und der ias AG ist unvollständig oder nicht konform mit Art. 28 DSGVO.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Hoch (Formeller Verstoß mit Bußgeldrisiko, unklare Haftungs- und Kontrollregelungen.)
- **Risikostufe: Hoch**

Risiko: Die ias AG setzt nicht genehmigte oder unzuverlässige Unterauftragsverarbeiter ein, wodurch der Arbeitgeber die Kontrolle über die Daten verliert.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Hoch (Verstoß gegen den AVV, Daten könnten unsicher oder zweckfremd verarbeitet werden.)
- **Risikostufe: Hoch**

4.2.7 Risiken bezüglich internationaler Datenübermittlung

Risiko: Personenbezogene Daten werden unbemerkt in ein Drittland ohne angemessenes Datenschutzniveau (z.B. USA) übermittelt, weil ein Unterauftragsverarbeiter dort ansässig ist.

- *Eintrittswahrscheinlichkeit:* Mittel
- *Schwere des Schadens:* Hoch (Verstoß gegen Kapitel V der DSGVO, Risiko des Zugriffs durch ausländische Behörden.)
- **Risikostufe: Hoch**

5 Geplante Abhilfemaßnahmen zur Risikobehandlung

Um die in Kapitel 5 identifizierten Risiken zu minimieren, sind die folgenden Abhilfemaßnahmen durch den Verantwortlichen (den Arbeitgeber) umzusetzen bzw. vom Auftragsverarbeiter (ias AG) einzufordern.

5.1 Maßnahmen bezüglich Rechtmäßigkeit und Legitimation

Sicherstellung der Freiwilligkeit:

- *Maßnahme 1:* Erstellung einer unternehmensweiten Kommunikationsrichtlinie, die klarstellt, dass die Nicht-Nutzung der App keinerlei Nachteile im Beschäftigungsverhältnis nach sich zieht. Aktive Kommunikation durch die Geschäftsführung.
- *Maßnahme 2:* Sofern ein Betriebsrat besteht, ist der Abschluss einer freiwilligen Betriebsvereinbarung (BV) zu prüfen, welche die Freiwilligkeit und die Rahmenbedingungen (z.B. Ausschluss leistungs- oder verhaltensbezogener Auswertungen) rechtsverbindlich festschreibt.

Gewährleistung einer informierten Einwilligung:

- *Maßnahme 3:* Überarbeitung der Einwilligungstexte und der Datenschutzerklärung nach dem Prinzip der einfachen und klaren Sprache (Art. 12 DSGVO). Es soll ein mehrschichtiges Informationsmodell ("Layered Approach") verwendet werden: eine kurze, prägnante Zusammenfassung vorab, gefolgt von der detaillierten Erklärung.

5.2 Maßnahmen bezüglich Zweckbindung, Datenqualität und Speicherbegrenzung

Sicherstellung einer wirksamen Anonymisierung:

- *Maßnahme 4:* Anforderung einer detaillierten Dokumentation des Anonymisierungsverfahrens von der ias AG. Vertragliche Festlegung im AVV, dass Statistiken nur bei

einer Mindestgruppengröße (z.B. nicht unter 10 Personen) erstellt werden dürfen, um eine De-Anonymisierung zu erschweren.

Umsetzung der Speicherbegrenzung:

- *Maßnahme 5:* Anforderung und Prüfung eines detaillierten Löschkonzepts der ias AG. Im AVV müssen konkrete Speicher- und Löschfristen für alle Datenkategorien (inkl. Backups) definiert werden.

5.3 Maßnahmen bezüglich Transparenz

Vollständige Information der Betroffenen:

- *Maßnahme 6:* Ergänzung der Datenschutzerklärung (Art. 13 DSGVO) um alle fehlenden Informationen, insbesondere: namentliche Nennung aller Unterauftragsverarbeiter, deren Standorte, und eine verständliche Erläuterung der Funktionsweise der statistischen Auswertungen.

5.4 Maßnahmen bezüglich Betroffenenrechte

Implementierung von Prozessen:

- *Maßnahme 7:* Einrichtung einer Funktion direkt in der App, über die Nutzer einfach und unkompliziert ihr Konto löschen (Recht auf Löschung) oder eine Auskunft über ihre Daten anfordern können.
- *Maßnahme 8:* Im AVV müssen klare Prozesse und Zuständigkeiten für die Bearbeitung von Betroffenenanfragen (Auskunft, Löschung etc.) definiert werden, um die Einhaltung der Monatsfrist (Art. 12 Abs. 3 DSGVO) zu gewährleisten.

5.5 Maßnahmen bezüglich Datensicherheit (TOMs)

Überprüfung und Sicherstellung eines hohen Sicherheitsniveaus:

- *Maßnahme 9:* Anforderung und eingehende Prüfung der vollständigen Dokumentation der Technischen und Organisatorischen Maßnahmen (TOMs) der ias AG gemäß Art. 32 DSGVO.
- *Maßnahme 10:* Anforderung von Nachweisen über die Wirksamkeit der TOMs, z.B. durch aktuelle Zertifizierungen (ISO 27001) oder die Vorlage von Ergebnissen externer Sicherheitsüberprüfungen (z.B. Penetrationstests).

5.6 Maßnahmen bezüglich Auftragsverarbeitung

Herstellung von Vertrags-Compliance:

- *Maßnahme 11:* Abschluss eines AVV, der allen Anforderungen des Art. 28 Abs. 3 DSGVO entspricht. Besonderes Augenmerk ist auf die Weisungsrechte, die Pflichten zur Unterstützung des Verantwortlichen und die Regelungen zu Unterauftragsverarbeitern zu legen.

- *Maßnahme 12:* Im AVV muss eine Klausel enthalten sein, die den Einsatz neuer oder den Wechsel von Unterauftragsverarbeitern von der vorherigen schriftlichen Genehmigung durch den Arbeitgeber abhängig macht.

5.7 Maßnahmen bezüglich internationaler Datenübermittlung

Verhinderung unzulässiger Drittlandtransfers:

- *Maßnahme 13:* Vertragliche Zusicherung im AVV einholen, dass eine Verarbeitung personenbezogener Daten ausschließlich innerhalb der EU/des EWR erfolgt. Jede beabsichtigte Änderung dieses Grundsatzes muss dem Arbeitgeber vorab zur Genehmigung vorgelegt werden und erfordert eine gesonderte Prüfung der Zulässigkeit (z.B. Abschluss von Standardvertragsklauseln plus Transfer-Impact-Assessment).

6 Bewertung des Restrisikos und Konsultation

7 Bewertung des Restrisikos und Konsultation

7.1 Bewertung des verbleibenden Risikos

Nach konsequenter Umsetzung der in Kapitel 6 beschriebenen Abhilfemaßnahmen werden die identifizierten Risiken signifikant reduziert. Dennoch verbleibt, insbesondere aufgrund der Verarbeitung von Gesundheitsdaten im Beschäftigungskontext, ein Restrisiko.

- **Risiko der unwirksamen Einwilligung (informeller Druck):**
  - *Bewertung:* Durch klare Kommunikation und eine mögliche Betriebsvereinbarung wird die Eintrittswahrscheinlichkeit stark gesenkt. Der potenzielle Schaden bleibt hoch.
  - **Restrisiko: Mittel**

- **Risiko der unzureichenden Anonymisierung:**
  - *Bewertung:* Durch vertragliche Vorgaben und die Prüfung des technischen Konzepts wird das Risiko minimiert. Die Schwere eines potenziellen Schadens bleibt jedoch sehr hoch.
  - **Restrisiko: Hoch** (Ein Restrisiko der De-Anonymisierung bei kleinen Gruppen oder durch Datenkombination kann nie vollständig ausgeschlossen werden.)

- **Risiko des unbefugten Zugriffs (Datensicherheit):**
  - *Bewertung:* Durch Prüfung der TOMs und vertragliche Garantien wird die Eintrittswahrscheinlichkeit gesenkt. Absolute Sicherheit gibt es jedoch nicht. Angesichts der Sensitivität von Gesundheitsdaten bleibt die Schadensschwere sehr hoch.
  - **Restrisiko: Hoch** (Das Risiko eines erfolgreichen, hochentwickelten Cyberangriffs bleibt bestehen.)

- **Risiko durch Auftragsverarbeitung und Drittlandtransfer:**
  - *Bewertung:* Durch einen konformen AVV und das vertragliche Verbot von Drittlandtransfers werden diese Risiken auf ein Minimum reduziert.
  - **Restrisiko: Niedrig**

Zusammenfassend lässt sich sagen, dass die organisatorischen und vertraglichen Risiken durch die Maßnahmen gut beherrschbar sind. Die verbleibenden Kernrisiken sind technischer Natur (Wirksamkeit der Anonymisierung und der Datensicherheit) und liegen im Wesen der Verarbeitung von Gesundheitsdaten begründet.

7.2 Ergebnis zur Notwendigkeit einer vorherigen Konsultation (Art. 36 DSGVO)

Gemäß Art. 36 Abs. 1 DSGVO muss der Verantwortliche die Aufsichtsbehörde konsultieren, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung – trotz der vom Verantwortlichen getroffenen Abhilfemaßnahmen – voraussichtlich ein hohes Risiko zur Folge hätte.

In der vorliegenden Bewertung verbleiben mindestens zwei Risiken (unzureichende Anonymisierung, unbefugter Zugriff) in der Kategorie "Hoch". Dies ist primär auf die extreme Schadensschwere zurückzuführen, die mit der Offenlegung von Gesundheitsdaten verbunden ist, selbst wenn die Eintrittswahrscheinlichkeit als gering bis mittel eingeschätzt wird.

Ergebnis: Aufgrund des verbleibenden hohen Risikos für die Rechte und Freiheiten der betroffenen Mitarbeiter wird die **vorherige Konsultation der zuständigen Aufsichtsbehörde** vor Beginn der Verarbeitung dringend empfohlen.

Dies dient nicht nur der Erfüllung der gesetzlichen Pflicht aus Art. 36 DSGVO, sondern auch der Rechtssicherheit für den Arbeitgeber. Die Aufsichtsbehörde kann die geplanten Maßnahmen bewerten und gegebenenfalls weitere, risikomindernde Auflagen machen, bevor die Verarbeitung beginnt.

8 Gesamtbewertung und Empfehlungen

8.1 Zusammenfassende Bewertung der Datenschutzkonformität

Der Einsatz der Gesundheitsapp „Mein ias“ ist **unter der Voraussetzung der vollständigen und konsequenten Umsetzung aller in Kapitel 6 genannten Abhilfemaßnahmen** datenschutzkonform möglich.

Das Fundament für einen rechtmäßigen Einsatz ist die uneingeschränkte Freiwilligkeit der Teilnahme. Sie ermöglicht die Einholung einer wirksamen Einwilligung als Rechtsgrundlage für die Verarbeitung der hochsensiblen Gesundheitsdaten (Art. 9 Abs. 2 lit. a DSGVO).

Dennoch verbleiben aufgrund der Art der Daten und des Beschäftigungskontextes hohe Risiken, die eine sorgfältige Steuerung und Kontrolle erfordern. Die Verantwortung des Arbeitgebers liegt insbesondere in der Auswahl und Überwachung des Auftragsverarbeiters (ias AG) sowie in der Sicherstellung eines transparenten und druckfreien Umfelds

für die Mitarbeiter. Die in dieser Datenschutz-Folgenabschätzung identifizierten Maßnahmen sind daher nicht optional, sondern zwingende Voraussetzung für einen rechtmäßigen Betrieb.

8.2 Konkrete Handlungsempfehlungen an die Geschäftsleitung

Vor der Einführung der App „Mein ias“ sind die folgenden Schritte in der angegebenen Priorität durchzuführen:

Priorität 1: Vertragliche und technische Grundlagen schaffen

- **Auftragsverarbeitungsvertrag (AVV) verhandeln und abschließen:** Fordern Sie von der ias AG einen AVV-Entwurf an und prüfen Sie diesen sorgfältig gegen die Anforderungen des Art. 28 DSGVO. Bestehen Sie auf der Umsetzung der in Kapitel 6 genannten Punkte (insb. Genehmigung von Unterauftragsverarbeitern, Weisungsrechte, Verbot von Drittlandtransfers). **Kein Einsatz der App ohne gültigen AVV!**
- **Technische Konzepte einfordern und prüfen:** Fordern Sie von der ias AG detaillierte, schriftliche Konzepte zu den Technischen und Organisatorischen Maßnahmen (TOMs), dem Anonymisierungsverfahren und dem Löschkonzept an. Bewerten Sie diese auf Angemessenheit und Wirksamkeit.
- **Datenschutzerklärung finalisieren:** Lassen Sie die Datenschutzerklärung für die App auf Basis der von der ias AG gelieferten Informationen erstellen und juristisch prüfen, um die Anforderungen der Art. 13 DSGVO vollständig zu erfüllen.

Priorität 2: Interne Organisation und Kommunikation sicherstellen

- **Kommunikationsstrategie entwickeln:** Planen Sie die interne Kommunikation an die Belegschaft. Betonen Sie klar und wiederholt die Freiwilligkeit der Teilnahme und dass aus einer Nicht-Nutzung keinerlei Nachteile entstehen.
- **Betriebsrat einbeziehen (falls vorhanden):** Suchen Sie frühzeitig das Gespräch mit dem Betriebsrat, um die Rahmenbedingungen in einer freiwilligen Betriebsvereinbarung zu regeln. Dies erhöht die Akzeptanz und schafft Rechtsicherheit.
- **Prozesse für Betroffenenrechte definieren:** Legen Sie intern fest, wie Anfragen von Mitarbeitern (Auskunft, Löschung etc.) kanalisiert und in Zusammenarbeit mit der ias AG fristgerecht bearbeitet werden.

Priorität 3: Behördliche Abstimmung (finaler Schritt)

- **Konsultation der Aufsichtsbehörde:** Führen Sie, wie in Kapitel 7 empfohlen, die vorherige Konsultation der zuständigen Datenschutz-Aufsichtsbehörde gemäß Art. 36 DSGVO durch. Reichen Sie dazu diese Datenschutz-Folgenabschätzung ein und warten Sie die Rückmeldung der Behörde ab, bevor die App für die Mitarbeiter freigeschaltet wird.