



KANZLEI KRÜGER
DATENSCHUTZ
COMPLIANCE
VERTRAGSRECHT

WHITEPAPER

WHITEPAPER ZUR VERORDNUNG (EU) 2016/679 DATENSCHUTZ- GRUNDVERORDNUNG

Ein Datenschutz-Leitfaden für die Einführung
einer Job-Rotation im Unternehmen



Inhalt

Inhalt	1
Einleitung	2
I. DATENSCHUTZ BEI EINEM ROTATIONSPROJEKT	3
1.1. Datenschutz als Erfolgsfaktor	3
1.2. Risiken bei unzureichendem Datenschutz	5
II. MAßNAHMENPLAN ZUM DATENSCHUTZ - ÜBERBLICK	6
2.1. Muster-Verarbeitung zur Auftragsverarbeitung.....	6
2.2. Auditierung der technischen und organisatorischen Maßnahmen.....	7
2.3. Verwendung dedizierter Zugangsdaten für jeden Berater.....	7
2.4. Privacy by Design: Anforderungen an die Systemgestaltung	8
III. Funktionalitäten und Datenschutzkonformität	9
3.1. Verantwortlichkeit für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten.....	10
3.2 Funktionalitäten und Bordwerkzeuge zur Wahrung von Betroffenenrechten.....	11
3.2.1. Recht auf Informationen bei Datenerhebung Art. 13 und 14 DSGVO	11
3.2.2. Recht auf Auskunft Art. 15 DSGVO	12
3.2.3. Recht auf Berichtigung Art. 16 DSGVO.....	12
3.2.4. Recht auf Vergessenwerden / Recht auf Löschung Art. 17 DSGVO	13
3.2.5. Recht auf Einschränkung der Verarbeitung Art. 18 DSGVO.....	14
3.2.6. Recht auf Datenübertragbarkeit Art. 20 DSGVO.....	14
3.2.7. Recht auf Widerspruch Art. 21 DSGVO	15
3.2.8. Zusammenfassung	15
IV. Änderungsprotokollierung der Verarbeitungsvorgänge	16
V. erstellung und führung eines verarbeitungsverzeichnis	16
VI. Durchführung einer Datenschutz-folgeabschätzung	17
VII. Erstellung eines Löschkonzepts	18
VIII. Fazit.....	19
Anhang 1 - Musterdatenschutzerklärung für Beschäftigte im Rahmen von Rotationsprojekten	20
Anhang 2 – Musterprozess für die Bearbeitung von Auskunftersuchen (Art. 15 DSGVO)	23
Anhang 3 - Musterprozess für die Bearbeitung von Löschanfragen (Art. 17 DSGVO).....	24
Anhang 4 – Musterprozess für die Bearbeitung von Widersprüchen (Art. 21 DSGVO)	25



EINLEITUNG

Rotationsprojekte erforschen neue Wege, wie systematischer Arbeitsplatzwechsel die Arbeitsorganisation verbessern und gleichzeitig die Zufriedenheit der Beschäftigten stärken kann. Dabei kommen auch moderne digitale Hilfsmittel wie Wearables oder Softwarelösungen zum Einsatz, die wertvolle Daten liefern, um den Rotationsprozess sinnvoll zu gestalten.

Gerade weil hierbei personenbezogene und zum Teil auch sensible Informationen verarbeitet werden, spielt Datenschutz eine entscheidende Rolle. Nur wenn die Vorgaben der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) konsequent eingehalten werden, können Rechtssicherheit und Vertrauen der Beschäftigten gewährleistet werden.

Dieser Leitfaden soll dabei unterstützen, die datenschutzrechtlichen Anforderungen eines Rotationsprojekts von Anfang an in die Planung und Umsetzung einzubeziehen. Er gibt einen Überblick über die zentralen Aspekte, die es zu beachten gilt, und zeigt praktische Maßnahmen auf, mit denen ein verantwortungsvoller und transparenter Umgang mit den erhobenen Daten sichergestellt werden kann.

Stand: Januar 2026

I. DATENSCHUTZ BEI EINEM ROTATIONSPROJEKT

Die Verarbeitung personenbezogener Daten spielt bei der automatisierten und optimierten Planung von Rotationsschichten eine unverzichtbare Rolle. Wer ein solches Projekt plant, sollte den Datenschutz daher von Anfang an als zentrales Gestaltungsprinzip berücksichtigen. Ziel muss es sein, die Vorteile einer intelligenten Schichtplanung bestmöglich zu nutzen und gleichzeitig sicherzustellen, dass die Rechte, Interessen und Erwartungen der Beschäftigten jederzeit gewahrt bleiben.

Ein datenschutzkonformes Rotationsprojekt erfordert die sorgfältige Abstimmung technischer, organisatorischer und rechtlicher Maßnahmen. Schon in der Planungsphase sollten Verantwortliche klare Strukturen schaffen, um den gesetzlichen Vorgaben der DSGVO gerecht zu werden und ein tragfähiges Fundament für die spätere praktische Umsetzung zu legen.

1.1. Datenschutz als Erfolgsfaktor

Grundsätze und Ziele

- Verankerung von Datenschutz als Qualitätsmerkmal und Bestandteil der Projekterfolgskriterien
- Ausrichtung an den Grundsätzen der DSGVO:
 - Zweckbindung
 - Datenminimierung
 - Richtigkeit
 - Speicherbegrenzung
 - Integrität und Vertraulichkeit
 - Rechenschaftspflicht
- Nachweisbare Rechtmäßigkeit der Verarbeitung durch klare Rechtsgrundlagen (z. B. Einwilligung, Vertragserfüllung, berechtigte Interessen mit Interessenabwägung)

Kernmaßnahmen

Maßnahme	Beschreibung
Privacy by Design	Frühzeitige Integration datenschutzrechtlicher Anforderungen in Architektur, Prozesse und Workflows, inklusive Risikoanalyse und ggf. Datenschutz-Folgenabschätzung

Privacy by Default	Grundlegender Ansatz, nur die für den jeweiligen Zweck notwendigen personenbezogenen Daten zu verarbeiten (rollenbasierter Zugriff, minimal erforderliche Felder, abgeschaltete Tracking-Funktionen).
Transparenz	Leicht zugängliche, verständliche Information für alle Beteiligten zu Zweck und Umfang der Datenverarbeitung(en), Kategorien von Daten, Empfänger, Speicherdauer und Rechte der Betroffenen etc.
Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)	Dokumentierte Prozesse, Verarbeitungsverzeichnisse, Löschkonzepte, Berechtigungskonzepte, technische und organisatorische Maßnahmen (TOM), Prüf- und Freigabeschritte
Vertrauensaufbau	Nachweis der Einhaltung gesetzlicher Vorgaben durch Audits, Prüfprotokolle, Schulungen und klare Beschwerde- und Feedbackkanäle

Organisatorische Umsetzung

- **Einbindung relevanter Stakeholder:** Frühzeitige Beteiligung von Betriebsrat, IT, HR und Datenschutzbeauftragten; Abstimmung zu Mitbestimmungsthemen und arbeitsorganisatorischen Auswirkungen
- **Governance:** Benennung von Verantwortlichkeiten (Projektleitung, Datenschutzbeauftragte/r, IT-Sicherheit), definierte Eskalations- und Freigabewege
- **Qualifizierung:** Schulungen für Projektteam und teilnehmende Beschäftigte zu Datenschutz, Datensicherheit und korrekter Nutzung der Systeme

Technische und prozessuale Sicherungen

Bereich	Maßnahmen
Datensicherheit	Verschlüsselung (Transport/Ruhe), Protokollierung und Monitoring, Zugriffsbeschränkungen, regelmäßige Sicherheitsupdates und Penetrationstests
Pseudonymisierung/Anonymisierung	Reduktion von Personenbezug, wo immer möglich; strikte Trennung von Identifikationsschlüsseln
Datenökonomie	Klare Zweckdefinition, Minimierung erhobener Merkmale, frühzeitige Löschung und Archivierung nach festgelegten Fristen

Externe Partner	Vertrags- und Auftragsverarbeitungsregelungen, Due-Diligence und Kontrollrechte bei Dienstleistern
------------------------	--

1.2. Risiken bei unzureichendem Datenschutz

Ein Rotationsprojekt ohne integriertes Datenschutzkonzept birgt erhebliche Risiken auf mehreren Ebenen.

Rechtliche und finanzielle Risiken

- **Bußgelder nach DSGVO:** Verstöße gegen die DSGVO können zu Bußgeldern von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes führen.
- **Informationspflichten:** Die Nichtbeachtung der Informationspflichten nach Art. 13, 14 DSGVO stellt einen eigenständigen Verstoß dar.
- **Vertragliche Mängel:** Fehlende oder mangelhafte Auftragsverarbeitungsverträge sowie unzureichende technische und organisatorische Maßnahmen (TOMs) führen zu rechtlicher Unsicherheit.

Vertrauen und Akzeptanz

Um die Mitwirkung und Bereitschaft zur Teilnahme bei den Projektteilnehmern sicherzustellen, sollten folgende Grundsätze beachtet werden:

Maßnahme	Wirkung
Klare Regeln gegen verdeckte Leistungs- und Verhaltenskontrollen	Keine automatisierten Entscheidungen ohne menschliche Bewertung
Privacy by Design/Default als Designprinzip	Datenschutz als Qualitätsmerkmal des gesamten Ansatzes
Vertrauensrahmen für Beschäftigte	Sicherheit, dass sensible Daten geschützt und nicht missbräuchlich verwendet werden
Transparente Datenverarbeitung	Stärkung der Akzeptanz des gesamten Rotationskonzepts
Nachvollziehbare Datenschutzmaßnahmen	Abbau von Befürchtungen vor Leistungs- und Verhaltenskontrolle
Aktive Förderung der Teilnahmebereitschaft	Hohes Engagement im Rotationsprozess

II. MAßNAHMENPLAN ZUM DATENSCHUTZ - ÜBERBLICK

Damit ein Rotationsprojekt rechtssicher und vertrauenswürdig umgesetzt werden kann, müssen die datenschutzrechtlichen Anforderungen von Beginn an in die Planung integriert werden. Entscheidend ist, dass sowohl die vertraglichen Rahmenbedingungen als auch die organisatorischen und technischen Schutzmaßnahmen so ausgestaltet sind, dass eine datenschutzkonforme Nutzung jederzeit gewährleistet ist. Gleichzeitig müssen Verantwortliche in der Lage sein, ihre Rechenschaftspflichten gemäß Art. 5 Abs. 2 DSGVO nachweisbar zu erfüllen.

Der folgende Abschnitt stellt die zentralen Bausteine eines Maßnahmenplans dar und gibt einen praxisnahen Überblick über die wesentlichen Schritte, die Verantwortliche im Rahmen eines Rotationsprojekts berücksichtigen sollten. Diese Bausteine dienen als Orientierung, wie Datenschutzanforderungen frühzeitig verankert und in der Praxis umgesetzt werden können.

2.1. Muster-Verarbeitung zur Auftragsverarbeitung

Nach den Vorgaben der DSGVO ist jeder Verantwortliche, der einen Auftragsverarbeiter für die Verarbeitung personenbezogener Daten einsetzt, verpflichtet, mit diesem einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO zu schließen. Dies betrifft insbesondere Dienstleistungen wie das Hosting oder den Support der Rotationssoftware. Eine solche Auftragsverarbeitung liegt zum Beispiel vor, wenn der Softwareanbieter die technische Bereitstellung und Wartung der Lösung übernimmt.

Um die rechtssichere Einbindung zu erleichtern, wurde im Rahmen des Projekts eine Mustervereinbarung zur Auftragsverarbeitung entwickelt. Diese kann von Verantwortlichen als Grundlage genutzt und an die spezifischen Gegebenheiten angepasst werden. Die Vereinbarung enthält eine klare Darstellung der Rechte und Pflichten beider Parteien sowie eine detaillierte Beschreibung der technischen und organisatorischen Maßnahmen (TOMs), die der Auftragsverarbeiter – und gegebenenfalls eingesetzte Unterauftragnehmer – zum Schutz personenbezogener Daten umzusetzen hat.

Für die Vertragspraxis sollten Verantwortliche insbesondere folgende Aspekte berücksichtigen:

- Klarstellung der Rollen und Verantwortlichkeiten: Wer ist Verantwortlicher, wer agiert als Auftragsverarbeiter?
- Verarbeitungsrahmen: Gegenstand, Dauer, Art und Zweck der Verarbeitung, Kategorien der betroffenen Personen sowie die betroffenen Datenarten.
- Weisungs- und Kontrollrechte: Der Verantwortliche muss das Recht haben, Weisungen zu erteilen und die Einhaltung der vereinbarten Maßnahmen regelmäßig zu überprüfen – etwa durch Audits oder geeignete Nachweise.
- Einsatz von Unterauftragnehmern: Diese dürfen nur nach vorheriger Genehmigung durch den Verantwortlichen eingesetzt werden. Transparenz über eingesetzte Dienstleister ist unverzichtbar.
- Technische und organisatorische Maßnahmen (TOMs): Es sollte eine detaillierte Beschreibung der Sicherheitsmaßnahmen vorliegen, die sich idealerweise an etablierten Standards wie ISO 27001 oder den IT-Grundschutz-Katalogen des BSI orientiert.

- Lösch- und Rückgaberegungen: Am Ende des Vertragsverhältnisses muss eindeutig festgelegt sein, ob die Daten gelöscht oder zurückgegeben werden.
- Vertraulichkeit: Mitarbeitende des Auftragsverarbeiters sind nachweislich zur Verschwiegenheit zu verpflichten.

Für die Praxis empfiehlt es sich, bereits vor Projektstart eine Mustervereinbarung zu entwickeln oder auf bewährte Vorlagen zurückzugreifen, die später an die konkreten Anforderungen des Projekts angepasst werden können. Dadurch lassen sich Abstimmungen mit den beteiligten Dienstleistern beschleunigen und typische Fehler vermeiden.

Darüber hinaus sollten Verantwortliche prüfen, ob der gewählte Auftragsverarbeiter regelmäßig Audits, Zertifizierungen oder Sicherheitsprüfungen vorweisen kann. Diese Nachweise erleichtern es, die eigene Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO zu erfüllen und gegenüber Aufsichtsbehörden oder internen Kontrollinstanzen belegen zu können, dass ein angemessenes Datenschutzniveau sichergestellt ist.

Wird ein Rotationsprojekt künftig in einer Organisation eingeführt, empfiehlt es sich daher, das Thema Auftragsverarbeitung frühzeitig in die Planungsphase einzubeziehen, um Rechtssicherheit zu schaffen und Vertrauen bei den Beschäftigten aufzubauen.

2.2. Auditierung der technischen und organisatorischen Maßnahmen

Die Wirksamkeit der vereinbarten technischen und organisatorischen Maßnahmen sollte nicht nur dokumentiert, sondern auch regelmäßig überprüft werden. Ein etabliertes Vorgehen ist die Durchführung unabhängiger Audits, die die tatsächliche Umsetzung der Vorgaben kontrollieren und in einem Prüfvermerk dokumentieren.

Dieser Prüfvermerk kann sowohl gegenüber internen Stakeholdern (z. B. Geschäftsführung, Betriebsrat, Datenschutzbeauftragter) als auch gegenüber Aufsichtsbehörden als Nachweis dienen, dass die Vorgaben aus Art. 24 Abs. 1 sowie Art. 28 Abs. 1 und 5 DSGVO eingehalten werden.

Für eine nachhaltige Absicherung empfiehlt es sich:

- Auditierungen in regelmäßigen Abständen zyklisch durchzuführen,
- Prozessbeschreibungen revisionssicher fortzuschreiben und zu aktualisieren,
- externe Audit-Dienstleister einzubeziehen, um ein objektives Prüfergebnis zu erhalten.

Sollte ein Rotationsprojekt in Zukunft auf weitere Anwendungsbereiche oder Unternehmen ausgeweitet werden, können auch diese von der vorhandenen Auditierung profitieren und – falls erforderlich – eigene Nachweise oder ergänzende Prüfungen anschließen.

2.3. Verwendung dedizierter Zugangsdaten für jeden Berater

Ein wesentlicher Baustein für die datenschutzkonforme Durchführung von Auftragsverarbeitungstätigkeiten ist der Einsatz individueller Zugangsdaten. Verantwortliche sollten sicherstellen, dass jede externe Person, die im Rahmen eines Rotationsprojekts Zugriff auf die Systeme erhält (z. B. Berater, Dienstleister oder Supportpersonal), separate und personalisierte Zugangsdaten nutzt.

Wichtige Punkte für die Umsetzung:

- **Individuelle Accounts:** Für jede externe Person muss ein eigenes Benutzerkonto eingerichtet werden. Gemeinsame Sammel-Accounts („Shared Accounts“) sind unbedingt zu vermeiden.
- **Sicherer Übermittlungsweg:** Zugangsdaten dürfen nicht per unverschlüsselter E-Mail oder auf unsicheren Kanälen bereitgestellt werden. Empfohlen werden abgestimmte Verfahren wie verschlüsselte Übertragung oder passwortgeschützte Dokumente mit separater Schlüsselübermittlung.
- **Technische Absicherung:** Zugangsdaten sollten in einer zentral administrierten Passwort- oder Zugangsdatenverwaltungssoftware abgelegt werden. Diese muss gewährleisten, dass nur autorisierte Personen Zugriff haben und die Einsichtnahme durch Unbefugte ausgeschlossen ist.
- **Protokollierung und Nachvollziehbarkeit:** Sämtliche Aktivitäten, die über die dedizierten Zugangsdaten erfolgen, sollten protokolliert werden (z. B. über Änderungsprotokolle oder Audit-Logs). Dadurch können Verantwortliche jederzeit prüfen, welche Verarbeitungsschritte von welcher Person vorgenommen wurden.

Durch den konsequenten Einsatz von dedizierten Zugangsdaten wird nicht nur das Risiko eines Missbrauchs erheblich reduziert, sondern auch die **Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO** unterstützt: Verantwortliche können im Bedarfsfall nachweisen, dass Zugriffe klar einer Person zugeordnet und kontrolliert sind.

2.4. Privacy by Design: Anforderungen an die Systemgestaltung

Das Prinzip „Privacy by Design“ gemäß Art. 25 DSGVO verlangt, dass Datenschutz bereits in der Konzeptions- und Entwicklungsphase eines Rotationsprojekts fest verankert wird. Dies bedeutet, dass die eingesetzten Systeme von Grund auf so gestaltet sein müssen, dass sie die Vorgaben der Datenschutz-Grundverordnung erfüllen. Dabei geht es nicht nur um technische Anpassungen, sondern auch um die Integration geeigneter Funktionen und Werkzeuge, die eine datenschutzkonforme Nutzung ermöglichen.

Kernfunktionen datenschutzkonformer Systeme

Um das Prinzip Privacy by Design umzusetzen, sollten die eingesetzten Systeme folgende Basisfunktionen bereitstellen:

Funktion	Beschreibung
Rollen- und Rechteverwaltung	Differenzierte Zugriffssteuerung, um den Zugang zu personenbezogenen Daten klar zu regeln
Protokollierung und Logging	Nachvollziehbarkeit aller Verarbeitungsschritte durch revisionssichere Dokumentation
Betroffenenrechte	Mechanismen zur Wahrung der Rechte (z. B. Datenexport für Auskunftersuchen, Lösch- und Korrekturmöglichkeiten)
Sicherheitsstandards	Verschlüsselung, Zwei-Faktor-Authentifizierung und sichere Schnittstellen

Von der Funktion zur datenschutzkonformen Nutzung

Die bloße Bereitstellung dieser Funktionen bedeutet noch nicht, dass automatisch eine DSGVO-konforme Nutzung erfolgt. Privacy by Design erfordert darüber hinaus, dass Verantwortliche durch gezieltes Customizing und die Einführung klar definierter, gesetzeskonformer Prozesse sicherstellen, dass die Systeme tatsächlich datenschutzgerecht eingesetzt werden.

Praxisempfehlungen

- **Softwareauswahl:** Bereits bei der Auswahl von Softwarelösungen für ein Rotationsprojekt sollte geprüft werden, ob diese die oben genannten Funktionen nativ bereitstellen
- **Einführungskonzept:** Verantwortliche sollten ein dokumentiertes Konzept entwickeln, das die Anpassung an die konkrete Unternehmensstruktur und die rechtlichen Anforderungen beschreibt
- **Protokollierung:** Eine vollständige Protokollierung aller Verarbeitungsvorgänge – beispielsweise über ein Modul für Änderungsprotokolle – sollte von Beginn an eingeplant werden, um die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erfüllen zu können

Mit der konsequenten Umsetzung von Privacy by Design wird gewährleistet, dass die Systeme nicht nur formal datenschutzkonform gestaltet sind, sondern in der praktischen Anwendung auch tatsächlich ein hohes Datenschutzniveau sichern.

Praxisempfehlung:

- Bereits bei der Auswahl von Softwarelösungen für ein Rotationsprojekt sollte geprüft werden, ob diese die oben genannten Funktionen bereitstellen („Privacy by Design“).
- Verantwortliche sollten ein **Einführungskonzept** entwickeln, das die Anpassung an die konkrete Unternehmensstruktur und die rechtlichen Anforderungen dokumentiert.
- Eine vollständige **Protokollierung aller Verarbeitungsvorgänge** – beispielsweise über ein Modul für Änderungsprotokolle – sollte von Beginn an eingeplant werden, um die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erfüllen zu können.

So wird gewährleistet, dass die Systeme nicht nur formal datenschutzkonform gestaltet sind, sondern in der praktischen Anwendung auch tatsächlich ein hohes Datenschutzniveau sichern.

III. FUNKTIONALITÄTEN UND DATENSCHUTZKONFORMITÄT

Dieser Abschnitt bietet einen kompakten Überblick über die datenschutzrechtlichen Anforderungen, die typischerweise bei der Einführung und Nutzung einer Unternehmenssoftware im Rahmen von Rotationsprojekten relevant sind. Gleichzeitig wird dargestellt, welche Funktionalitäten eine geeignete Softwarelösung mitbringen sollte, um die Umsetzung dieser Anforderungen zu unterstützen.



Bei der Auswahl und Implementierung einer Softwarelösung für Rotationsprojekte ist darauf zu achten, dass diese die gesetzlichen Datenschutzvorgaben vollständig abbilden kann. Dies ermöglicht eine datenschutzkonforme Nutzung und erleichtert die Einhaltung der Rechenschaftspflichten gemäß DSGVO und BDSG, insbesondere bei der Erfassung, Verarbeitung und Speicherung personenbezogener Daten.

Für Unternehmen, die Rotationsprojekte implementieren möchten, sollte eine geeignete Softwarelösung folgende Funktionen bereitstellen, um alle datenschutzrechtlichen Anforderungen wirksam umzusetzen:

- Betroffenenrechte: Mechanismen zur einfachen Wahrnehmung und Bearbeitung von Auskunfts-, Berichtigungs-, Lösungs- und Widerspruchsanfragen
- Protokollierung: Detaillierte und revisionssichere Dokumentation aller Verarbeitungsvorgänge
- Zugriffs- und Rechteverwaltung: Sichere, rollenbasierte Berechtigungskonzepte zur Einschränkung des Datenzugriffs auf befugte Personen

3.1. Verantwortlichkeit für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Grundsätzlich liegt die Verantwortung für die Einhaltung der datenschutzrechtlichen Grundsätze bei jedem Unternehmen oder jeder Einrichtung, die personenbezogene Daten verarbeitet (Verantwortlicher im Sinne der DSGVO). Dies umfasst sowohl organisatorische und prozessuale Maßnahmen als auch die korrekte Parametrierung und Rechteverwaltung der eingesetzten Softwareanwendungen. Software-Anbieter stellen die notwendigen Funktionen und Tools bereit, um diese Anforderungen technisch zu unterstützen. Die datenschutzrechtliche Verantwortung für die tatsächliche Umsetzung der DSGVO-Konformität bleibt jedoch beim jeweiligen Verantwortlichen.

Praxisbeispiel:

Eine zentrale Voraussetzung für die Rechtmäßigkeit der Datenverarbeitung ist das Vorliegen einer der in Art. 6 DSGVO genannten Grundlagen. Im Rahmen von Rotationsprojekten können dabei insbesondere folgende Grundlagen relevant sein:

Rechtsgrundlage	Beschreibung
Art. 6 Abs. 1 lit. a DSGVO	Einwilligung der betroffenen Person
§ 26 Abs. 2 BDSG	Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung
Art. 9 Abs. 2 lit. a DSGVO	Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten

Grundsätze der ordnungsgemäßen Datenverarbeitung

Die genannten Verantwortlichkeiten gelten auch für alle Grundsätze der ordnungsgemäßen Datenverarbeitung:

- **Zweckbindung:** Personenbezogene Daten dürfen nur für die festgelegten Zwecke verarbeitet werden
- **Datenminimierung:** Die Verarbeitung der Daten muss auf das notwendige Maß beschränkt sein
- **Richtigkeit der Daten:** Unrichtige personenbezogene Daten müssen unverzüglich korrigiert werden

Die Umsetzung dieser Prinzipien ist überwiegend prozessualer Natur und kann nicht vollständig automatisiert von einer Software übernommen werden. Eine geeignete Softwarelösung für Rotationsprojekte sollte jedoch Werkzeuge bereitstellen, die ein hohes Datenschutzniveau unterstützen und eine nachvollziehbare Umsetzung ermöglichen.

3.2 Funktionalitäten und Bordwerkzeuge zur Wahrung von Betroffenenrechten

Ein zentrales Ziel bei der Einführung und Nutzung datenschutzkonformer Rotations-Management-Software ist die Sicherstellung der Betroffenenrechte nach den Artikeln 13 bis 21 DSGVO. Diese Rechte stellen ein wesentliches Instrument dar, um Transparenz zu gewährleisten und das Vertrauen der Beschäftigten in die eingesetzten Systeme zu stärken.

Im Folgenden werden die einzelnen Rechte dargestellt, jeweils mit Hinweisen zu praxisgerechten Umsetzungsschritten, die in Projekten oder in Unternehmen berücksichtigt werden sollten. Ergänzend finden Sie Hinweise auf Mustertexte und Vorlagen (s. Anhang), die eine einheitliche und rechtssichere Bearbeitung erleichtern.

3.2.1. Recht auf Informationen bei Datenerhebung | Art. 13 und 14 DSGVO

Beschäftigte müssen zum Zeitpunkt der Datenerhebung über Art, Umfang und Zweck der Verarbeitung informiert werden. Erfolgt die Datenerhebung nicht unmittelbar bei der betroffenen Person, sind die Informationspflichten nach Art. 14 DSGVO zu beachten.

Praxis-Umsetzung:

- Erstellung einer standardisierten **Datenschutzerklärung für Beschäftigte** mit allen erforderlichen Angaben (z. B. Kategorien der verarbeiteten Daten, Zwecke, Rechtsgrundlagen, Empfänger, Speicherdauer, Hinweis auf Betroffenenrechte)
- Hinterlegung dieser Erklärung sowohl digital (z. B. im Mitarbeiterportal) als auch in Papierform (z. B. Arbeitsvertrag)
- Regelmäßige Aktualisierung der Datenschutzhinweise bei Änderungen der Verarbeitungsprozesse

Unterstützung durch die Software:

Eine geeignete Software sollte folgende Funktionen bereitstellen:

- Möglichkeit, Dokumente oder Links zu Datenschutzhinweisen bei der Registrierung im System anzuzeigen
- Automatisierte Bestätigungsabfrage („Informationen gelesen und verstanden“) bei der ersten Anmeldung

Hinweis: Die in Anhang 1 dargestellten Muster-Datenschutzhinweise können als Vorlage genutzt werden. Diese sollten an die spezifischen Verarbeitungsprozesse im jeweiligen Unternehmen oder der jeweiligen Einrichtung angepasst werden.

3.2.2. Recht auf Auskunft | Art. 15 DSGVO

Beschäftigte haben ein Recht darauf zu erfahren, ob und welche personenbezogenen Daten über sie gespeichert werden, einschließlich der Kategorien von Empfängern und der Verarbeitungszwecke (Art. 15 DSGVO).

Praxis-Umsetzung:

- Einrichtung eines definierten Prozesses, wie Auskunftsanfragen entgegengenommen, geprüft und beantwortet werden
- Einhaltung der standardisierten Frist: grundsätzlich innerhalb eines Monats nach Antragstellung
- Dokumentation des Ablaufs: (Eingang der Anfrage, Bearbeitungsschritte, Ergebnis)

Unterstützung durch die Softwarelösung:

Funktion	Nutzen
Exportfunktion	Export personenbezogener Daten in gängigem, strukturiertem Format zur Beantwortung von Auskunftersuchen
Änderungsprotokolle	Nachvollziehbarkeit der Verarbeitung belegen
Getrennte Zugänge	Einbindung separater Berater- oder Administratorzugänge zur Verhinderung von Missbrauch

Hinweis: In Anhang 2 ist ein beispielhafter Ablaufplan für den Umgang mit Auskunftsanträgen enthalten, der als Vorlage für die Prozessgestaltung dienen kann.

3.2.3. Recht auf Berichtigung | Art. 16 DSGVO

Betroffene können verlangen, dass unrichtige Daten korrigiert oder unvollständige Daten ergänzt werden.

Praxis-Umsetzung

- Definition eines Workflows für die Entgegennahme und Prüfung von Berichtigungsanträgen
- Sicherstellung, dass alle Änderungen protokolliert und dokumentiert werden
- Festlegung von Zuständigkeiten und Fristen für die Bearbeitung

Unterstützung durch Softwarelösungen

Eine geeignete Software sollte folgende Funktionen bereitstellen:

Funktion	Nutzen
Editierbare Stammdatenfelder	Alle relevanten personenbezogenen Daten können bei Bedarf korrigiert oder ergänzt werden
Änderungsvermerke	Dokumentation, wann und von wem Änderungen vorgenommen wurden
Prüfverläufe	Nachvollziehbarkeit aller Bearbeitungsschritte zur Erfüllung der Rechenschaftspflicht

3.2.4. Recht auf Vergessenwerden / Recht auf Löschung | Art. 17 DSGVO

Unter bestimmten Voraussetzungen (z. B. Widerruf einer Einwilligung, Zweckfortfall) können Beschäftigte die Löschung ihrer personenbezogenen Daten verlangen.

Praxis-Umsetzung

- Erstellung eines Löschkonzepts, das Fristen für unterschiedliche Datenarten definiert:
 - bspw. Arbeitszeitdaten, Qualifikationsdaten, Fotos, weitere personenbezogene Daten
- Unterscheidung zwischen Daten, die sofort zu löschen sind, und solchen, die aufgrund gesetzlicher Aufbewahrungspflichten weiterhin gespeichert werden müssen
- Dokumentation jeder Löschung:
 - Wer hat die Löschung durchgeführt?
 - Was wurde gelöscht?
 - Wann erfolgte die Löschung?

Unterstützung durch Softwarelösungen

Eine geeignete Software sollte folgende Funktionen bereitstellen:

Funktion	Nutzen
Automatische Löschung/Anonymisierung	Regelbasierte Löschung oder Anonymisierung nach Ablauf definierter Fristen
Manuelle Löschung	Option zur gezielten Löschung einzelner Datensätze bei berechtigten Anträgen

Hinweis: In Anhang 3 ist ein Leitfaden für die praktische Umsetzung von Löschanträgen enthalten, der als Vorlage für die Prozessgestaltung dienen kann.

3.2.5. Recht auf Einschränkung der Verarbeitung | Art. 18 DSGVO

Beschäftigte können die Einschränkung der Verarbeitung verlangen, z. B. während einer Prüfung der Richtigkeit der Daten oder bei einem eingeleiteten Widerspruch.

Praxis-Umsetzung

- Definition eines Prozesses, wie Daten im System „eingefroren“ werden können, ohne sie zu löschen
- Interne Kennzeichnung, dass die Daten zwar gespeichert, aber nicht weiter genutzt werden dürfen
- Festlegung von Zuständigkeiten für die Bearbeitung entsprechender Anträge

Unterstützung durch Softwarelösung

Eine geeignete Software sollte folgende Funktionen bereitstellen:

Funktion	Nutzen
Sperrfunktion	Möglichkeit zur Sperrung einzelner Datensätze oder ganzer Benutzerkonten
Protokollierung	Dokumentation, wann und durch wen die Einschränkung vorgenommen oder aufgehoben wurde

3.2.6. Recht auf Datenübertragbarkeit | Art. 20 DSGVO

Beschäftigte können verlangen, ihre Daten in einem gängigen, maschinenlesbaren Format zu erhalten oder direkt an einen anderen Verantwortlichen übermitteln zu lassen.

Praxis-Umsetzung

- Implementierung einer Routine, die Anträge auf Datenübertragbarkeit prüft und fristgerecht umsetzt
- Sicherstellung, dass der Export vollständig und datenschutzkonform erfolgt (z. B. Verschlüsselung bei Übertragung)
- Dokumentation der durchgeführten Datenübertragungen

Unterstützung durch Softwarelösungen

Eine geeignete Software sollte folgende Funktionen bereitstellen:

Funktion	Nutzen
Exportfunktion	Export in standardisierten, maschinenlesbaren Formaten wie CSV, XML oder JSON
Sicherer Versandkanal	Verschlüsselte E-Mail oder Download über geschützten Bereich zur datenschutzkonformen Übermittlung

3.2.7. Recht auf Widerspruch | Art. 21 DSGVO

Betroffene Personen haben nach Art. 21 DSGVO grundsätzlich das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen, wenn diese auf Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse) oder Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) gestützt wird.

Relevanz im Kontext eines Rotationsprojekts

In der praktischen Umsetzung von Rotationsprojekten ist dieses Recht in der Regel von untergeordneter Bedeutung. Das liegt daran, dass die Verarbeitung personenbezogener Daten überwiegend auf anderen Rechtsgrundlagen erfolgt:

Rechtsgrundlage	Anwendungsbereich
Art. 6 Abs. 1 lit. a DSGVO	Einwilligung der betroffenen Person
§ 26 Abs. 2 BDSG	Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung
Art. 9 Abs. 2 lit. a DSGVO	Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten

Da auf Einwilligung gestützte Verarbeitungen nicht vom Widerspruchsrecht nach Art. 21 DSGVO erfasst sind, können Beschäftigte insoweit keinen Widerspruch einlegen. Stattdessen steht ihnen das Recht zu, ihre Einwilligung jederzeit zu widerrufen (Art. 7 Abs. 3 DSGVO).

Praktische Empfehlungen

- Beschäftigte sollten im Rahmen der Datenschutzhinweise transparent darauf hingewiesen werden, in welchen Fällen ein Widerspruch nach Art. 21 DSGVO möglich ist und in welchen Fällen stattdessen ein Widerruf der Einwilligung in Betracht kommt
- Sollte im Einzelfall eine Verarbeitung tatsächlich auf Art. 6 Abs. 1 lit. f DSGVO beruhen (z. B. optionale Auswertungen zur Optimierung von Schichtmodellen), muss ein eingehender Widerspruch sorgfältig geprüft und dokumentiert werden
- Für diese Fälle empfiehlt sich die Festlegung eines klaren Prozesses zur Bearbeitung von Widersprüchen:
 - Dokumentation des Eingangs und der Bearbeitungsschritte
 - Rückmeldung an die betroffene Person

3.2.8. Zusammenfassung

Die Wahrung der Betroffenenrechte ist nicht allein eine technische Frage, sondern erfordert immer ein Zusammenspiel von Softwarefunktionen und organisatorischen Prozessen. Während die Software durch Bordwerkzeuge (z. B. Export, Protokollierung, Sperrung) wichtige Unterstützung leistet, bleibt die Verantwortung für die vollständige und fristgerechte Umsetzung stets beim Verantwortlichen.

IV. ÄNDERUNGSPROTOKOLLIERUNG DER VERARBEITUNGSVORGÄNGE

Grundsätzlich ist eine Protokollierung sämtlicher Verarbeitungsvorgänge gesetzlich nicht vorgeschrieben. § 76 BDSG verpflichtet jedoch alle Verantwortlichen und Auftragsverarbeiter, bei automatisierten Verarbeitungsvorgängen, zur Protokollierung bestimmter Verarbeitungsvorgänge.

Unabhängig davon kann eine Änderungsprotokollierung jedoch eine geeignete Maßnahme nach Art. 32 DSGVO sein, um die Rechenschaftspflicht zu unterstützen und den Nachweis datenschutzkonformer Verarbeitung zu erleichtern.

Wird eine Protokollierung eingeführt, sollte sie mindestens folgende Angaben enthalten: wer (Benutzerkennung), wann (Zeitpunkt), welche Aktion (z. B. Änderung, Löschung, Export) und in welchem Systembereich. Protokolle sind vor unbefugtem Zugriff zu schützen, dürfen nur berechtigten Personen zugänglich sein und müssen nach angemessenen Fristen gelöscht werden.

Für Unternehmen empfiehlt es sich, im Auftragsverarbeitungsvertrag mit Dienstleistern klar zu regeln, ob und wie eine Protokollierung erfolgt. Ein optionales Modul zur Änderungsprotokollierung kann dabei helfen, Nachvollziehbarkeit zu schaffen und Verantwortlichkeiten im Bedarfsfall eindeutig zuzuordnen.

V. ERSTELLUNG UND FÜHRUNG EINES VERARBEITUNGSVERZEICHNISSES

Nach Art. 30 DSGVO sind Unternehmen und Einrichtungen verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Diese Pflicht gilt grundsätzlich ab 250 Beschäftigten. Bei kleineren Organisationen besteht sie ebenfalls, wenn:

- die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
- die Verarbeitung nicht nur gelegentlich erfolgt, oder
- besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) bzw. Daten zu Straftaten (Art. 10 DSGVO) verarbeitet werden.

Pflichtangaben im Verzeichnis

Das Verzeichnis muss mindestens folgende Angaben enthalten:

Angabe	Beschreibung
Verantwortlicher	Name und Kontaktdaten (ggf. auch gemeinsam Verantwortlicher, Vertreter und Datenschutzbeauftragter)
Verarbeitungszwecke	Zwecke der Verarbeitung
Betroffene Personen	Kategorien betroffener Personen und Kategorien personenbezogener Daten

Empfänger	Kategorien von Empfängern (inkl. Drittländer oder internationale Organisationen)
Drittlandübermittlung	Ggf. Datenübermittlungen an Drittländer mit Angabe der Garantien
Löschfristen	Löschfristen für die einzelnen Datenkategorien
TOMs	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 DSGVO)

Für die Praxis empfiehlt es sich, das Verzeichnis in tabellarischer Form anzulegen, um Übersichtlichkeit und Aktualisierbarkeit zu gewährleisten.

VI. DURCHFÜHRUNG EINER DATENSCHUTZ-FOLGEABSCHÄTZUNG

Nach Art. 35 DSGVO müssen Unternehmen und Einrichtungen eine Datenschutz-Folgenabschätzung (DSFA) durchführen, wenn eine geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Dies ist insbesondere der Fall bei:

- umfangreicher oder systematischer Überwachung,
- Verarbeitung großer Mengen besonders sensibler Daten (z. B. Gesundheitsdaten),
- automatisierten Bewertungen oder Profiling,
- Einsatz neuer Technologien, deren Auswirkungen noch nicht absehbar sind.

Praktische Empfehlungen

Die Entscheidung über die Erforderlichkeit einer DSFA sollte nachvollziehbar dokumentiert werden – auch wenn keine DSFA durchgeführt wird. Hilfreiche Orientierung bieten:

- Blacklists der Datenschutzaufsichtsbehörden
- Empfehlungen der zuständigen Aufsichtsbehörden
- Leitlinien des Europäischen Datenschutzausschusses (EDSA)

VII. ERSTELLUNG EINES LÖSCHKONZEPTS

Jedes Unternehmen ist nach Art. 5 Abs. 1 lit. e DSGVO verpflichtet, personenbezogene Daten nur so lange zu speichern, wie es für die Zwecke ihrer Verarbeitung erforderlich ist. Daraus ergibt sich die Pflicht, ein unternehmensspezifisches Löschkonzept zu entwickeln und konsequent umzusetzen.

Bestandteile eines Löschkonzepts

Ein Löschkonzept für Rotationsprojekte sollte insbesondere folgende Punkte berücksichtigen:

Bestandteil	Beschreibung
Differenzierte Löschfristen	Für jede Kategorie personenbezogener Daten (z. B. Arbeitszeitdaten, Qualifikationsdaten, Einsatzpläne) müssen individuelle Lösch- oder Anonymisierungsfristen festgelegt werden
Rechtsgrundlagen	Bei der Definition der Fristen sind gesetzliche Aufbewahrungspflichten (z. B. aus dem Arbeitsrecht, Steuerrecht oder Sozialversicherungsrecht) sowie tarifliche, betriebliche oder vertragliche Vorgaben einzubeziehen
Dokumentation	Das Konzept sollte nachvollziehbar dokumentieren, welche Daten wann und auf welcher Grundlage gelöscht werden
Technische Umsetzung	Die Software sollte Funktionen bereitstellen, die eine automatisierte oder halbautomatisierte Löschung nach Ablauf der Fristen unterstützen
Regelmäßige Überprüfung	Das Konzept ist in festgelegten Abständen zu überprüfen und bei geänderten gesetzlichen oder organisatorischen Anforderungen anzupassen

Nutzen eines strukturierten Löschkonzepts

Ein klar strukturiertes Löschkonzept trägt nicht nur zur Einhaltung der DSGVO bei, sondern stärkt auch das Vertrauen der Beschäftigten, da deren Daten nicht länger als nötig gespeichert werden.



VIII. FAZIT

Der vorliegende Leitfaden zeigt, dass die datenschutzkonforme Umsetzung eines Rotationsprojekts von Beginn an systematisch geplant werden muss. Die Verarbeitung personenbezogener Daten ist ein zentraler Bestandteil der automatisierten Planung und der Optimierung von Rotationsprozessen. Nur durch konsequente Berücksichtigung der gesetzlichen Vorgaben der DSGVO und des BDSG kann Rechtssicherheit geschaffen und das Vertrauen der Beschäftigten gewahrt werden.

Wesentliche Erfolgsfaktoren

Ein strukturierter Maßnahmenplan, der sowohl organisatorische als auch technische Aspekte berücksichtigt, ist unerlässlich. Wesentliche Elemente sind:

Element	Beschreibung
Verzeichnis der Verarbeitungstätigkeiten	Dokumentation aller Verarbeitungsvorgänge gemäß Art. 30 DSGVO
Zugangsmangement	Implementierung dedizierter Zugangsdaten und rollenbasierter Berechtigungen
Betroffenenrechte	Berücksichtigung und Umsetzung aller Rechte nach Art. 15–21 DSGVO
Regelmäßige Audits	Durchführung von Prüfungen zur Sicherstellung der Datenschutzkonformität
Löschkonzept	Einführung eines strukturierten Konzepts zur fristgerechten Datenlöschung

Anhang 1 - Musterdatenschutzerklärung für Beschäftigte im Rahmen von Rotationsprojekten

1. Verantwortlicher und Datenschutzbeauftragter

Verantwortlicher:

[Name des Unternehmens/der Einrichtung]

[Vollständige Adresse]

[Telefonnummer]

[E-Mail-Adresse]

Datenschutzbeauftragter:

[Name]

[Kontaktdaten]

E-Mail: [datenschutz@unternehmen.de]

2. Zweck und Rechtsgrundlage der Datenverarbeitung

Ihre personenbezogenen Daten werden zu folgenden Zwecken verarbeitet:

- Aufzeigen von Möglichkeiten der Reduktion von Überbelastungen
- Entwicklung eines Rotationsplans basierend auf der tatsächlichen körperlichen Belastung
- Eruierung der Belastungen/ Auslastungen am Arbeitsplatz
- Schichtplanung und Rotations-Management zur optimalen Personaleinsatzplanung und Arbeitsorganisation
- Analyse von Arbeitsplatzanforderungen und individuellen Qualifikationen zur bestmöglichen Zuordnung
- Überwachung und Bewertung der Rotationseffekte zur kontinuierlichen Verbesserung der Arbeitsorganisation
- Gesundheitsförderung und Präventionsmaßnahmen durch ergonomische Optimierung der Arbeitsplätze

Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. a DSGVO - (Einwilligung)
- § 26 Abs. 2 BDSG – (Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung)
- Art. 9 Abs. 2 lit. a DSGVO – (Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten)

3. Kategorien verarbeiteter personenbezogener Daten

- Demografische Daten
 - Alter, Geschlecht, Händigkeit, Größe, Gewicht, Muttersprache, Bildungsstand, Berufstätigkeit, Deutschkenntnisse

- Substanzeinnahmen (Medikamente, Drogen, Nikotin), Erkrankungen (Herz-Kreislauf, neurologisch, psychisch, muskel-skelettal), Koffeinkonsum, sportliche Tätigkeiten
- Stammdaten der Mitarbeiter (Name, Vorname, Position)
- Vitaldaten (Puls, Herzratenvariabilität, elektrodermale Aktivität)

4. Empfänger oder Kategorien von Empfängern

Ihre Daten können an folgende Stellen weitergegeben werden:

- **Interne Bereiche:** Personalabteilung, direkte Vorgesetzte, Betriebsrat (soweit mitbestimmungspflichtig)
- **Externe Dienstleister:** IT-Dienstleister, Beratungsunternehmen (nur bei entsprechenden Auftragsverarbeitungsverträgen)

5. Dauer der Speicherung

- **Arbeitszeitdaten:** Aufbewahrung gemäß § 16 Abs. 2 Arbeitszeitgesetz für mindestens 2 Jahre
- **Aktive Rotationsphase:** Planungs- und Analysedaten werden für die Dauer der aktiven Rotation gespeichert
- **Evaluierungsdaten:** 3 Jahre nach Abschluss der Rotationsmaßnahme zur Bewertung der Langzeiteffekte
- **Einwilligungsbasierte Daten:** Löschung bei Widerruf, spätestens bei Beendigung des Arbeitsverhältnisses

6. Ihre Rechte als betroffene Person

Sie haben folgende Rechte:

- **Auskunftsrecht (Art. 15 DSGVO):** Auskunft über die Sie betreffenden verarbeiteten Daten
- **Berichtigungsrecht (Art. 16 DSGVO):** Korrektur unrichtiger Daten
- **Löschungsrecht (Art. 17 DSGVO):** Löschung unter bestimmten Voraussetzungen
- **Einschränkungsrecht (Art. 18 DSGVO):** Einschränkung der Verarbeitung
- **Datenübertragbarkeit (Art. 20 DSGVO):** Übertragung Ihrer Daten in strukturierter Form
- **Widerspruchsrecht (Art. 21 DSGVO):** Widerspruch gegen die Verarbeitung bei berechtigten Interessen

7. Widerruf von Einwilligungen

Soweit die Verarbeitung auf Ihrer Einwilligung beruht, können Sie diese jederzeit widerrufen. Der Widerruf berührt nicht die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung.

8. Beschwerderecht

Sie haben das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten zu beschweren.

Zuständige Aufsichtsbehörde:

[Name und Kontaktdaten der zuständigen Landesbehörde]

9. Automatisierte Entscheidungsfindung

VARIANTE A:

Im Rahmen der automatisierten Schichtplanung und Job-Rotation können automatisierte Verfahren eingesetzt werden, die auf folgenden Parametern basieren:

- **Schichtplanungsalgorithmen:** Berücksichtigung von Arbeitszeiten, Qualifikationen und gesetzlichen Vorgaben
- **Rotationsempfehlungen:** Abgleich von Arbeitsplatzanforderungen mit individuellen Kompetenzen und Präferenzen
- **Optimierungsverfahren:** Effiziente Personalverteilung unter Berücksichtigung betrieblicher und individueller Faktoren

Sie haben das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen zu werden. Endgültige Rotations- und Schichtplanungsentscheidungen werden immer unter Einbeziehung menschlicher Bewertung getroffen.

VARIANTE B: Ohne automatisierte Entscheidungsfindung

Eine automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO findet nicht statt. Alle Entscheidungen im Rahmen des Rotationsprojekts – insbesondere zur Planung und Zuweisung von Arbeitsplätzen – werden ausschließlich unter Einbeziehung menschlicher Bewertung getroffen.

10. Freiwilligkeit und Auswirkungen

Die Teilnahme an der Job-Rotation ist grundsätzlich freiwillig. Eine Verweigerung hat keine negativen Auswirkungen auf Ihr Arbeitsverhältnis.

Anhang 2 – Musterprozess für die Bearbeitung von Auskunftersuchen (Art. 15 DSGVO)

Bearbeitung von Auskunftersuchen gemäß Art. 15 DSGVO:

- **Anfrage erfassen:**

- Jede Auskunftsanfrage wird schriftlich oder elektronisch erfasst und mit einem eindeutigen Vorgangskennzeichen versehen.
- Dokumentieren Sie: Datum, Name, Kontakt und Art der Anfrage
- Vor der Weitergabe von personenbezogenen Daten wird die Identität des Anfragenden geprüft. Bei Bedarf holen Sie mehr Informationen zur Klärung der Identität des Betroffenen ein.
- Versenden Sie eine Eingangsbestätigung an den Betroffenen und beachten Sie die 1-Monats-Frist ab Eingang.
- Informieren Sie Ihren Datenschutzbeauftragten sowie, falls notwendig, die betroffenen Abteilungen.

- **Daten recherchieren:**

Alle relevanten Daten, die im Rahmen der Rotationsplanung verarbeitet werden, werden in den eingesetzten Systemen (z. B. Rotationssoftware) gesammelt. Hierbei sind Änderungsprotokolle und separate Zugangsdaten zu berücksichtigen, um die vollständige Historie der Verarbeitung sicherzustellen.

- **Prüfung der Daten:**

Prüfen, ob bspw. vertragliche Pflichten die Herausgabe einzelner Daten einschränken.

Vollständigkeit und Richtigkeit prüfen.

Abgrenzung, ob Rechte Dritter betroffen sind (ggf. Schwärzungen).

- **Antwort erstellen:**

Die betroffene Person erhält eine Übersicht aller verarbeiteten personenbezogenen Daten sowie Informationen zu Zweck, Empfängern, Speicherdauer und den ihr zustehenden Rechten.

Form: Schriftlich oder elektronisch (sicheres Medium, z. B. verschlüsselte E-Mail oder per Post und in einem gängigen Format (z.B. PDF, CSV)

- **Dokumentation:**

Alle Schritte der Bearbeitung werden revisionssicher dokumentiert, um Nachweisbarkeit gegenüber Aufsichtsbehörden zu gewährleisten.

Anhang 3 - Musterprozess für die Bearbeitung von Löschanfragen (Art. 17 DSGVO)

Anfrage erfassen:

Jede Löschanfrage wird schriftlich oder elektronisch erfasst und mit einem eindeutigen Vorgangskennzeichen versehen.

Identität prüfen:

Vor der Löschung wird die Identität der anfragenden Person geprüft. Bei Bedarf holen Sie mehr Informationen zur Klärung der Identität des Betroffenen ein.

Rechtsgrundlage prüfen:

Prüfen, ob die Löschung rechtlich zulässig ist (z. B. kein Widerspruch gegen gesetzliche Aufbewahrungsfristen, Arbeitsrecht oder andere gesetzliche Pflichten).

Datenlokalisierung:

Alle personenbezogenen Daten, die gelöscht werden sollen, werden in den eingesetzten Systemen identifiziert, einschließlich Backup- und Archivsystemen.

Löschung durchführen:

Daten werden vollständig gelöscht oder anonymisiert, soweit dies technisch möglich und datenschutzrechtlich zulässig ist.

Bestätigung:

Die betroffene Person erhält eine Bestätigung der erfolgten Löschung oder eine Begründung, falls die Löschung nicht durchgeführt werden kann.

Dokumentation:

Der gesamte Prozess wird revisionssicher dokumentiert, um die Nachweisbarkeit gegenüber Aufsichtsbehörden zu gewährleisten.

Anhang 4 – Musterprozess für die Bearbeitung von Widersprüchen (Art. 21 DSGVO)

Anfrage erfassen:

Jeder Widerspruch gegen die Verarbeitung personenbezogener Daten wird schriftlich oder elektronisch entgegengenommen, erfasst und mit einem eindeutigen Vorgangskennzeichen versehen.

Identität prüfen:

Vor der Löschung wird die Identität der anfragenden Person geprüft. Bei Bedarf holen Sie mehr Informationen zur Klärung der Identität des Betroffenen ein.

Prüfung des Anwendungsfalls:

Da das Widerspruchsrecht in Art. 21 DSGVO nur in bestimmten Fällen greift, ist zu prüfen, ob die Datenverarbeitung auf Art. 6 Abs. 1 e) DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse) oder Art. 6 Abs. 1 f) DSGVO (berechtigte Interessen) gestützt wird.

Liegt eine Verarbeitung auf Grundlage von Einwilligung (Art. 6 Abs. 1 a) DSGVO) oder Vertrag (Art. 6 Abs. 1 b) DSGVO) vor, ist das Widerspruchsrecht in der Regel nicht einschlägig.

Interessenabwägung durchführen:

Wenn ein Widerspruch gegen eine Verarbeitung auf Grundlage von berechtigten Interessen eingeht, ist eine Abwägung zwischen den Interessen des Unternehmens und den Grundrechten der betroffenen Person vorzunehmen.

Ergibt die Abwägung, dass die Interessen der betroffenen Person überwiegen, ist die Verarbeitung einzustellen.

Bestehen zwingende schutzwürdige Gründe für die Verarbeitung, darf diese fortgesetzt werden, muss jedoch gut dokumentiert und begründet werden.

Kommunikation mit der betroffenen Person:

Die betroffene Person ist über das Ergebnis der Prüfung und die weitere Vorgehensweise schriftlich zu informieren.

Dokumentation:

Der gesamte Prozess – inklusive Begründung, Abwägungsergebnis und Kommunikation – wird revisionssicher dokumentiert, um die Nachweisbarkeit gegenüber Aufsichtsbehörden zu gewährleisten.

Fristen beachten:

Die Bearbeitung des Widerspruchs erfolgt unverzüglich und spätestens innerhalb eines Monats. Bei komplexen Fällen kann diese Frist verlängert werden, wobei die betroffene Person rechtzeitig informiert werden muss.