GRAFT

GDPR TEMPLATE PACK

Betriebsratspaket — Graft Workflow-Analyse (Deutschland)

Informationspaket für den Betriebsrat zur Einführung der Graft Workflow-Analyse. Erklärt Zweck, Datenumfang, Aggregation und Widerspruchsrechte.

VERSION	LAST UPDATED	PUBLISHED BY
v1.0	**2026-04-07**	**Graft**

TEMPLATE — REQUIRES LEGAL REVIEW BEFORE USE

This document is a drafting aid. Your DPO, legal counsel or works council should review every section before use.

> **WARNING**
> **Template -- requires legal review and native German review before publication.** This document was drafted in German by a non-native speaker. Before distribution, it must be reviewed by qualified German-language counsel and by the works council (Betriebsrat) of the deploying organisation. Terminology from BetrVG must be verified against current case law.

1. Zweck dieses Dokuments

Dieses Dokument informiert den Betriebsrat über die geplante Einführung der **Graft Workflow-Analyse** bei `<<KUNDE: Name des Unternehmens>>`. Es dient als Grundlage für die Mitbestimmung nach **§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG)** und ist Bestandteil der Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO.

Ziel der Analyse ist die Identifizierung von Arbeitsprozessen, die sich automatisieren oder vereinfachen lassen -- **nicht** die Leistungs- oder Verhaltenskontrolle einzelner Beschäftigter.

2. Was ist die Graft Workflow-Analyse?

Graft verbindet sich über **schreibgeschützte OAuth-Schnittstellen** mit den bereits im Unternehmen eingesetzten Arbeits-Tools -- typischerweise Jira, Microsoft 365 und Google Workspace -- und erstellt aus den **Metadaten** dieser Systeme eine aggregierte Landkarte der Arbeitsabläufe.

Die Analyse läuft üblicherweise für einen Zeitraum von 14 Tagen. Das Ergebnis ist ein Bericht an die Unternehmensleitung und, falls vereinbart, an den Betriebsrat. Der Bericht zeigt Muster auf Teamebene, nicht auf Einzelebene.

3. Was wird erfasst -- und was nicht?

Erfasst (Metadaten)	Nicht erfasst
Anzahl bearbeiteter Jira-Vorgänge pro Team und Tag	Inhalte von Jira-Vorgängen (Beschreibung, Kommentare)
Aktivitätszählungen aus Microsoft Graph Reports API (z. B. Anzahl gesendeter E-Mails)	Betreff, Inhalt, Empfänger oder Anhänge von E-Mails
Audit-Events aus Google Workspace Reports API (z. B. "Datei geöffnet")	Inhalte von Drive-Dokumenten, Gmail, Meet-Aufnahmen
Zeitstempel von Tool-Wechseln (z. B. Jira ’ Slack)	Bildschirminhalte, Tastatureingaben, Browser-Verlauf
Anonymisierte (gehashte) Nutzer-IDs zur internen Zuordnung	Klarnamen oder E-Mail-Adressen außerhalb des Quell-Systems

Kurzfassung: Graft erfasst, _was_ in welchen Tools passiert (Ereignisse, Zählungen, Wechsel), aber **niemals** _Inhalte_ oder _Kommunikation zwischen einzelnen Personen_.

4. Garantie aggregierter Verarbeitung

Alle Auswertungen werden grundsätzlich für Kohorten von **mindestens fünf Beschäftigten** (n >= 5) erstellt. Kleinere Gruppen werden im Bericht unterdrückt. Diese Schwelle ist im Produkt technisch erzwungen und kann vom Kunden nur nach oben, nicht nach unten angepasst werden.

Eine individuelle Auswertung einzelner Beschäftigter ist im Produkt **nicht vorgesehen** und vertraglich zwischen `<<KUNDE>>` und Graft **ausgeschlossen**. Die entsprechende Zusage ist in Abschnitt 4.2 des Auftragsverarbeitungsvertrags festgehalten.

5. Rechtsgrundlage und Datenschutz-Folgenabschätzung

Die Verarbeitung stützt sich auf **Art. 6 Abs. 1 lit. f DSGVO** (berechtigte Interessen). Einwilligung wird ausdrücklich **nicht** als Rechtsgrundlage herangezogen -- die Europäischen Datenschutzaufsichtsbehörden (EDSA-Leitlinien 05/2020) und Erwägungsgrund 43 DSGVO stellen klar, dass Einwilligung im Beschäftigungsverhältnis wegen des Machtungleichgewichts in der Regel nicht freiwillig ist.

Eine vollständige Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO liegt vor und wird dem Betriebsrat im Rahmen dieses Verfahrens zur Verfügung gestellt. Sie enthält eine dokumentierte Abwägung der Interessen (Legitimate Interests Assessment, LIA).

6. Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG

Die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, unterliegt der Mitbestimmung des Betriebsrats. Auch wenn Graft **nicht** zur Leistungs- oder Verhaltenskontrolle eingesetzt werden soll, ist das Tool nach ständiger Rechtsprechung des Bundesarbeitsgerichts **objektiv geeignet**, ein solches Verhalten zumindest theoretisch abzubilden. Damit greift das Mitbestimmungsrecht.

Wir bitten den Betriebsrat daher um Zustimmung zum Abschluss einer **Betriebsvereinbarung** zur Einführung der Graft Workflow-Analyse. Ein Entwurf liegt diesem Paket bei.

Die Betriebsvereinbarung sollte mindestens enthalten:

- Zweckbindung (ausschließlich Prozessoptimierung, keine Leistungs- oder Verhaltenskontrolle)
- Den Umfang der erfassten Daten (Metadaten, keine Inhalte)
- Die Aggregationsregel (n >= 5)
- Das Widerspruchsrecht (siehe Abschnitt 7)
- Die Aufbewahrungsfristen (90 Tage Rohdaten, 2 Jahre aggregierte Ergebnisse)
- Die Löschverpflichtung am Ende der Laufzeit
- Die Mitwirkungsrechte des Betriebsrats bei jeder wesentlichen Änderung des Verfahrens

7. Widerspruchsrecht

Beschäftigte können jederzeit und ohne Angabe von Gründen gegen die Einbeziehung in die Analyse widersprechen. Der Widerspruch ist zu richten an:

> **NOTE**
> `<<KUNDE: Kontakt-E-Mail für Widerspruch>>`

Der Widerspruch wird **innerhalb von 24 Stunden** bei der nächsten Synchronisation wirksam. Die Ausübung des Widerspruchsrechts ist **sanktionsfrei** und darf sich in keiner Weise nachteilig auf das Arbeitsverhältnis auswirken.

Der Widerspruch umfasst:

- Entfernung der gehashten Nutzer-ID und aller damit verknüpften Ereignisse
- Ausschluss aus allen zukünftigen Synchronisationen und Auswertungen

Bereits in aggregierten Berichten enthaltene anonymisierte Muster werden davon nicht berührt, da sie keinen Personenbezug mehr aufweisen.

8. Aufbewahrungsfristen

Datenklasse	Aufbewahrungsfrist	Löschmechanismus
Rohe Ereignisdaten	**90 Tage** ab Erfassung	Automatisierter täglicher Löschauftrag
Aggregierte Kohorten-Ergebnisse (n e 5, ohne Personenbezug)	**2 Jahre** ab Erfassung	Manuelle Löschung am Ende der Frist
OAuth-Zugangstoken	Bis zum Ende der Beauftragung oder zum Widerruf	Sofortige Löschung bei Widerruf

9. Sicherheitsmaßnahmen (Kurzfassung)

- Verschlüsselung in der Übertragung: TLS 1.2 oder höher
- Verschlüsselung bei Speicherung: AES-256-GCM (verwaltet über Nango)
- Mandantentrennung auf Anwendungsebene
- Mehrfaktorauthentifizierung für alle Kundenadministrator- und Graft-Mitarbeiter-Zugänge
- Audit-Protokollierung jeder Abfrage, die auf Nutzerebene ausgewertet werden könnte
- Meldefrist bei Datenpannen: **72 Stunden** gemäß Art. 33 DSGVO

Eine ausführliche Darstellung findet sich in Anlage 2 des Auftragsverarbeitungsvertrags.

10. Ansprechpersonen

Rolle	Kontakt

Datenschutzbeauftragte/r (Kunde)	`<<KUNDE: Name, E-Mail>>`
Betriebsratsvorsitzende/r	`<<KUNDE: Name, E-Mail>>`
Projektleitung (Kunde)	`<<KUNDE: Name, E-Mail>>`
Graft Datenschutz	`legal@graft.bot`
Zuständige Aufsichtsbehörde	`<<KUNDE: zuständige Landesdatenschutzbehörde>>`

11. Zustimmung des Betriebsrats

Rolle	Name	Unterschrift	Datum
Vorsitzende/r des Betriebsrats	`<<KUNDE>>`		
Stellvertretende/r Vorsitzende/r	`<<KUNDE>>`		
Datenschutzbeauftragte/r	`<<KUNDE>>`		

Dokumentenkontrolle

Feld	Wert
Version	1.0
Letzte Aktualisierung	2026-04-07
Nächste Überprüfung	2027-04-07 oder bei wesentlicher Änderung
Quelle	Graft GDPR template pack v1.0

Änderungsprotokoll

Version	Datum	Autor	Änderung
1.0	2026-04-07	Graft	Erstveröffentlichung