DPIA — workflow report

Generated by the Ansvar MCP Gateway workflow engine · 2026-05-14T10:04:39.897461+00:00 · workflow id `7a051f04-c91f-47a2-9346-b636dd522a82`

Processing under assessment

HR SaaS vendor 'PeopleFlow' processing payroll, performance reviews, absence data (incl. medical certificates), 'flight-risk' profiling for 1,200 employees across DE/NL/SE. US-based vendor, SCCs in place, sub-processor list includes AWS us-east-1 + analytics provider.

Screening — Article 35(3)

Outcome: DPIA required

Three Article 35(3) triggers fire concurrently: (a) systematic and extensive evaluation based on automated processing including 'flight-risk' profiling that materially affects employment decisions; (b) large-scale processing of special categories — medical certificates fall under Art. 9(1) health data — across 1,200 employees in three Member States; and (c) per the WP29 nine-criteria guidance adopted by EDPB, the combination of employee-context (vulnerable data subjects), large scale, sensitive data, evaluation/scoring, and international transfer crosses multiple thresholds. DE BfDI and NL AP mandatory DPIA lists both flag employee monitoring + profiling as triggering.

Criterion	Article	Description
Profiling with significant effect	GDPR Art. 35(3)(a)	Flight-risk score drives retention interventions, performance management cycles, succession planning — significantly affects the employee.
Large-scale special-category data	GDPR Art. 35(3)(b) + Art. 9(1)	Medical certificates (health data) for 1,200 employees across DE/NL/SE.
WP29 nine-criteria — employees as vulnerable data subjects	WP248 rev.01 (endorsed by EDPB)	Power asymmetry in employment context elevates risk.
Mandatory list — DE BfDI	BDSG §67 + BfDI Liste	Employee monitoring + behavioural profiling on the DE mandatory list.
Mandatory list — NL AP	AP Besluit DPIA-plichtig	Large-scale employee monitoring listed.

DPO consultation — Article 35(2)

- **Designated:** True
- **Advice sought:** True on 2026-05-08
- **Recommendation:** Proceed with DPIA; do not deploy flight-risk in production until Article 22 safeguards and TIA supplementary measures are in place.
- **Followed:** True

Advice summary. DPO recommended (i) treating flight-risk as Article 22 automated decision-making with meaningful human review before any retention intervention; (ii) supplementary technical measures on top of SCCs for US transfers per EDPB Recommendations 01/2020 (encryption-at-rest with EU-held keys, pseudonymisation of identifiers before transfer); (iii) Article 88 Member-State carve-outs to be honoured — BDSG §26 (DE), UAVG art. 30 (NL), Diskrimineringslagen + Sjuklagen (SE); (iv) works-council/employee-representative consultation before go-live in DE and NL.

Processing description

Purposes:

- Operate payroll and statutory reporting
- Track absence and leave entitlement
- Run performance review cycles
- Predict flight-risk to inform retention interventions
- Workforce planning and headcount analytics

Data types:

Category	Sensitivity	Art 9	Retention	Volume
Identity and contact	normal	—	employment + 10y (tax)	1200
Payroll (bank account, salary, tax ID)	financial	—	employment + 10y	1200
Performance reviews + manager comments	evaluative	—	employment + 3y	1200
Absence and leave	normal	—	employment + 5y	1200
Medical certificates (sick notes)	special	health	employment + 5y	1200
Flight-risk score and feature vector	derived/profiling	—	rolling 24m	1200

Legal basis. Art. 6: 6(1)(b) contract for payroll/performance; 6(1)(c) legal obligation for tax + sickness reporting; 6(1)(f) legitimate interest for flight-risk — contested, see risk assessment
Art. 9: 9(2)(b) employment, social security and social protection law — with Member-State carve-outs in BDSG §26 (DE), UAVG art. 30 (NL), and Diskrimineringslagen + Sjuklagen (SE)
Art. 10: N/A — no criminal-conviction data

Processors:

Processor	Country	Role
PeopleFlow Inc.	US	primary processor
AWS (us-east-1)	US	sub-processor — hosting
Analytics Inc.	US	sub-processor — ML feature pipeline

International transfers:

Destination	Mechanism
US	SCCs (Module 2 controller-to-processor, 2021/914) + transfer impact assessment under Schrems II
US	EU-US Data Privacy Framework — PeopleFlow self-certified; reliance pending TIA review

High-risk indicators — 8 of 9 present:

ID	Indicator	Present	Rationale
HRI-01	Evaluation/scoring (WP248)	yes	Flight-risk score affects retention/promotion.
HRI-02	Automated decision with legal/significant effect	yes	Score informs retention interventions and PIP triggers.
HRI-03	Systematic monitoring	yes	Continuous behavioural signal collection (login cadence, absence pattern, review tone).
HRI-04	Sensitive or special-category data	yes	Health data via medical certificates.

ID	Indicator	Present	Rationale
HRI-05	Data processed on a large scale	yes	1,200 subjects × 7 data types × 3 jurisdictions.
HRI-06	Matching/combining datasets	yes	Performance + absence + payroll combined into flight-risk feature vector.
HRI-07	Data on vulnerable subjects	yes	Employees in power-asymmetric relationship.
HRI-08	Innovative technology	no	Standard supervised ML — not novel.
HRI-09	Prevents data subjects from exercising a right or using a service	yes	Score may gate access to internal mobility programmes.

Necessity and proportionality

Necessity. Payroll, statutory absence reporting, and performance management are necessary for the employment contract and for legal obligations under DE/NL/SE tax + social security law. The flight-risk profiling purpose is not necessary for the contract; it is pursued on Article 6(1)(f) legitimate interest, which fails the balancing test for several feature inputs (manager-comment sentiment scoring, absence frequency as a flight-risk signal).

Proportionality. Categories 1–4 are proportionate. Category 5 (medical certificates) is proportionate only when stored as a hash + metadata for absence-entitlement enforcement; the current vendor design ingests the full certificate body, which is disproportionate. Category 6 (flight-risk feature vector) is disproportionate as designed — includes inputs (sick-leave count, manager-comment sentiment) that elevate Art. 22 risk without commensurate benefit.

Data minimisation. Strip free-text manager-comment ingestion; pseudonymise identifiers before transfer to PeopleFlow; restrict medical-certificate processing to entitlement check only (do not pass body to ML pipeline).

LIA outcome. LIA fails for the as-designed feature set; mitigation must drop the failing features or add Art. 22 safeguards including meaningful human review and opt-out.

Data-subject views — Article 35(9)

Sought: True

Method. Works-council briefing in DE (Betriebsrat) and NL (OR); anonymous employee survey in SE (n=312 responses, 26% response rate); 1-hour Q&A with employee-representative group across all three jurisdictions.

Summary. DE Betriebsrat objected to flight-risk profiling on Mitbestimmungspflicht grounds (BetrVG §87). NL OR requested clarification of human-review mechanism. SE survey: 71% uncomfortable with sentiment-on-manager-comments; 84% wanted opt-out; 92% wanted access to their score and reasoning. Cross-cutting themes: distrust of black-box scoring, concern about sick-leave used as a flight-risk signal, request for explicit human override.

Risk catalog (CNIL severity × likelihood)

Total: 0 risks. Residual matrix: 12 low / 0 medium / **0 high** / **0 critical**

ID	Description	Likelihood	Severity	Score	Residual
R-10	DE works-council co-determination right (BetrVG §87) not honoured before deployment of behavioural monitoring system.	**maximum (4)**	**significant (3)**	12	4
R-06	Sick-leave count used as flight-risk feature — indirect special-category processing of health data outside the Art. 9(2)(b) employment-law carve-out.	**maximum (4)**	**significant (3)**	12	2
R-02				9	4

ID	Description	Likelihood	Severity	Score	Residual
	Discriminatory or otherwise unfair flight-risk score produced by ML model trained on biased historical retention data.	**significant (3)**	**significant (3)**		
R-03	International transfer to US without effective safeguards — government access to data under FISA 702 / EO 12333 even with SCCs in place.	**significant (3)**	**significant (3)**	9	4
R-01	Unauthorised disclosure of medical certificates via PeopleFlow document store misconfiguration or sub-processor breach.	limited (2)	**significant (3)**	6	3
R-04	Function-creep: flight-risk score reused for layoff selection or compensation decisions beyond original purpose.	**significant (3)**	limited (2)	6	2
R-05	Manager-comment sentiment scoring captures subjective evaluative language and turns it into a quantified signal employees cannot effectively rebut.	**significant (3)**	limited (2)	6	2
R-09	Privacy notice does not explain the flight-risk logic, significance, and envisaged consequences (Art. 13(2)(f) / 14(2)(g)).	**significant (3)**	limited (2)	6	2
R-07	Data subject rights (access, erasure, objection, Art. 22 human-review) cannot be effectively exercised against a US processor at the technical layer.	limited (2)	limited (2)	4	2
R-08	Excessive retention of feature vectors (rolling 24m) accumulates a longitudinal profile beyond minimisation principle.	limited (2)	limited (2)	4	2
R-11	Sub-processor list change (PeopleFlow swaps analytics vendor) without controller approval breaks Art. 28(2) chain.	limited (2)	limited (2)	4	2
R-12	Insufficient logging of access to flight-risk scores by HR business partners and managers.	limited (2)	limited (2)	4	2

Per-risk safeguards

R-10 — DE works-council co-determination right (BetrVG §87) not honoured before deployment of behavioural monitoring system.

Likelihood: **maximum (4)** · Severity: **significant (3)** · Score: 12 → Residual: 4

Likelihood justification. DE Betriebsrat already objected; deployment without Betriebsvereinbarung is non-starter.

Severity justification. Supervisory authority can order halt; collective action; reputational damage internally.

#	Measure	Type	Article	Effort	Before → After
1	Negotiate Betriebsvereinbarung covering data categories, retention, access, and Art. 22 safeguards before any DE go-live. Mirror for NL OR.	organisational	Art. 88 + BDSG §26	high	12 → 4
2	SE jurisdiction proceeds in parallel only after SE union (Unionen) sign-off on the score reasoning + opt-out mechanism.	organisational	Art. 88 + Diskrimineringslagen	medium	9 → 4

R-06 — Sick-leave count used as flight-risk feature — indirect special-category processing of health data outside the Art. 9(2)(b) employment-law carve-out.

Likelihood: **maximum (4)** · Severity: **significant (3)** · Score: 12 → Residual: 2

Likelihood justification. Sick-leave count is already in the planned feature set; if shipped as designed this risk is certain.

Severity justification. Indirect special-category processing; sickness becomes a career penalty signal contrary to Recital 35 and Art. 9 carve-out scope.

#	Measure	Type	Article	Effort	Before → After
1	Remove sick-leave count from the feature vector entirely; replace with role-tenure and engagement-survey opt-in signals.	technical	Art. 9(1) + Art. 5(1)(c)	low	12 → 3
2	Document the feature-exclusion policy in the DPIA so future model retraining cannot silently re-add it.	organisational	Art. 5(2) accountability	low	6 → 2

R-02 — Discriminatory or otherwise unfair flight-risk score produced by ML model trained on biased historical retention data.

Likelihood: **significant (3)** · Severity: **significant (3)** · Score: 9 → Residual: 4

Likelihood justification. Historical retention data reflects existing demographic skew; supervised models replay it. Vendor has no documented bias-mitigation pipeline.

Severity justification. Discriminatory output silently shapes career outcomes; significant non-material harm to affected groups; potential collective claim risk under EU Charter Art. 21.

#	Measure	Type	Article	Effort	Before → After
1	Pre-deployment fairness audit (demographic parity + equalised odds) per gender, age band, jurisdiction; published bias-mitigation report.	organisational	Art. 35(7)(d)	high	12 → 6
2	Article 22 safeguard: meaningful human review before any retention intervention; documented override authority; employee right to contest.	organisational	Art. 22(3)	medium	12 → 4
3	Drop manager-comment sentiment scoring and sick-leave count from the feature set.	technical	Art. 5(1)(c)	low	9 → 4

R-03 — International transfer to US without effective safeguards — government access to data under FISA 702 / EO 12333 even with SCCs in place.

Likelihood: **significant (3)** · Severity: **significant (3)** · Score: 9 → Residual: 4

Likelihood justification. US is not adequate post-Schrems II without DPF reliance; PeopleFlow's DPF self-certification mitigates but does not eliminate FISA 702 exposure for the specific data categories.

Severity justification. Government access to health + behavioural data has no effective remedy for the data subject in the US.

#	Measure	Type	Article	Effort	Before → After
1	Supplementary technical measures per EDPB Recommendations 01/2020: encryption-at-rest with EU-held keys; pseudonymisation of identifiers (employee number, not name) before transfer.	technical	Art. 46	medium	12 → 6
2	Transfer Impact Assessment (TIA) documented per EDPB methodology; re-run on any sub-processor change or DPF status change.	organisational	Art. 46 + EDPB Rec. 01/2020	medium	9 → 6
3	Module 2 SCCs Clauses 14 + 15 obligations explicitly in DPA; vendor onward-disclosure notice within 72h.	contractual	Art. 28 + 46(2)(c)	low	6 → 4

R-01 — Unauthorised disclosure of medical certificates via PeopleFlow document store misconfiguration or sub-processor breach.

Likelihood: limited (2) · Severity: **significant (3)** · Score: 6 → Residual: 3

Likelihood justification. PeopleFlow has SOC 2 Type II + ISO 27001; AWS us-east-1 is mature; primary vector is misconfiguration of customer-managed access lists.

Severity justification. Health data of 1,200 employees; per Recital 75 health-data disclosure produces significant harm. Multi-jurisdiction notification under Art. 33/34.

#	Measure	Type	Article	Effort	Before → After
1	Customer-managed encryption keys (CMK) on the medical-certificate object store; envelope encryption with HSM-held KEK; document body encrypted before upload.	technical	Art. 32(1)(a)	medium	12 → 4
2	Restrict medical-certificate ingestion to hash + entitlement metadata; do not pass body to ML pipeline.	organisational	Art. 5(1)(c)	low	12 → 3
3	DPA Annex II TOMs review on PeopleFlow + sub-processors annually; pen-test of document-store ACLs.	contractual	Art. 28(3)(c)	low	6 → 3

R-04 — Function-creep: flight-risk score reused for layoff selection or compensation decisions beyond original purpose.

Likelihood: **significant (3)** · Severity: limited (2) · Score: 6 → Residual: 2

Likelihood justification. Score is attractive for unrelated HR decisions; pressure to reuse during workforce reductions is predictable.

Severity justification. Reusing the score for layoff selection would compound R-02 harm; isolated reuse limited in severity unless paired with discrimination.

#	Measure	Type	Article	Effort	Before → After
1	Purpose-binding policy: flight-risk score may not be used for compensation, layoff selection, or disciplinary action. Written into HR policy + DPA scope.	organisational	Art. 5(1)(b)	low	6 → 2
2	Access control: HR business partners only; managers see retention recommendation, not raw score.	technical	Art. 5(1)(f) + Art. 32	medium	6 → 3

R-05 — Manager-comment sentiment scoring captures subjective evaluative language and turns it into a quantified signal employees cannot effectively rebut.

Likelihood: **significant (3)** · Severity: limited (2) · Score: 6 → Residual: 2

Likelihood justification. Sentiment scoring is in PeopleFlow's standard pipeline; opaque to data subject by default.

Severity justification. Indirect effect on career outcomes; recoverable if score is removed and human review applied.

#	Measure	Type	Article	Effort	Before → After
1	Disable sentiment-on-manager-comments feature; if retained, expose the underlying classification to the employee on request with appeal route.	technical	Art. 16 + Art. 22(3)	low	6 → 2
2		organisational	Art. 5(1)(d)	low	4 → 2

#	Measure	Type	Article	Effort	Before → After
	Train managers on factual review-writing (vs. evaluative sentiment) so the underlying inputs are less amplified by sentiment scoring downstream.				

R-09 — Privacy notice does not explain the flight-risk logic, significance, and envisaged consequences (Art. 13(2)(f) / 14(2)(g)).

Likelihood: **significant (3)** · Severity: limited (2) · Score: 6 → Residual: 2

Likelihood justification. Existing privacy notice is generic HR-vendor language; doesn't address Art. 22.

Severity justification. Procedural breach with cascading effect on rights exercise, but readily remediable.

#	Measure	Type	Article	Effort	Before → After
1	Updated privacy notice with a dedicated section on flight-risk processing: logic in plain language, significance, envisaged consequences, contestation process.	organisational	Arts. 13(2)(f) + 14(2)(g)	low	6 → 2
2	Layered notice: short summary card surfaced in HR portal at first login; detailed annex for download.	organisational	Art. 12(1)	low	4 → 2

R-07 — Data subject rights (access, erasure, objection, Art. 22 human-review) cannot be effectively exercised against a US processor at the technical layer.

Likelihood: limited (2) · Severity: limited (2) · Score: 4 → Residual: 2

Likelihood justification. Vendor offers a DSAR endpoint; in practice latency and completeness for derived data (flight-risk score) are unknown.

Severity justification. Recoverable through controller-side workflow; supervisory authority can compel.

#	Measure	Type	Article	Effort	Before → After
1	Controller-hosted DSAR endpoint that proxies vendor and includes the flight-risk score + feature vector + logic explanation in the response.	technical	Arts. 15–22	medium	6 → 2
2	DPA SLA: vendor responds within 14 days to DSAR forwards.	contractual	Art. 28(3)(e)	low	4 → 2

R-08 — Excessive retention of feature vectors (rolling 24m) accumulates a longitudinal profile beyond minimisation principle.

Likelihood: limited (2) · Severity: limited (2) · Score: 4 → Residual: 2

Likelihood justification. Vendor default; not adversarial.

Severity justification. Storage limitation violation; magnifies impact of any other risk over time.

#	Measure	Type	Article	Effort	Before → After
1	Reduce feature-vector retention from rolling 24m to rolling 12m; auto-purge stale vectors on a monthly job.	technical	Art. 5(1)(e)	low	4 → 2
2	Document the retention rationale in the ROPA entry; review at every model retraining cycle.	organisational	Art. 30	low	4 → 2

R-11 — Sub-processor list change (PeopleFlow swaps analytics vendor) without controller approval breaks Art. 28(2) chain.

Likelihood: limited (2) · Severity: limited (2) · Score: 4 → Residual: 2

Likelihood justification. PeopleFlow has a sub-processor notification mechanism; risk is mainly notification-window lag.

Severity justification. Recoverable; documentary breach unless the new sub-processor introduces a separate risk.

#	Measure	Type	Article	Effort	Before → After
1	DPA clause requiring 30-day prior notice of sub-processor changes with controller's right to object; objection-without-resolution = termination right.	contractual	Art. 28(2) + 28(4)	low	4 → 2
2	Quarterly sub-processor review by the DPO; cross-check against EDPB Recommendations + DPF list status.	organisational	Art. 5(2)	low	4 → 2

R-12 — Insufficient logging of access to flight-risk scores by HR business partners and managers.

Likelihood: limited (2) · Severity: limited (2) · Score: 4 → Residual: 2

Likelihood justification. Vendor offers an audit log; controller has not yet validated coverage on per-employee score-access events.

Severity justification. Limits ability to evidence misuse; weakens Art. 5(2) defensibility.

#	Measure	Type	Article	Effort	Before → After
1	Enable per-employee, per-actor access logs on flight-risk score views; ship logs to controller SIEM via daily export.	technical	Art. 5(1)(f) + Art. 32(1)(d)	medium	4 → 2
2	Quarterly access-log review by the DPO; sampling-based anomaly check.	organisational	Art. 5(2)	low	4 → 2

Transfer compliance — Articles 44–49

Destination	Mechanism	Adequate	Note
US (PeopleFlow)	Module 2 SCCs (2021/914) + supplementary measures (encryption at rest with EU-held keys, pseudonymisation pre-transfer) + TIA documented	no	US is not adequate. SCCs alone insufficient post-Schrems II; supplementary measures bridge the gap. DPF self-certification by PeopleFlow noted as a parallel mechanism but TIA covers both paths.
US (AWS us-east-1 sub-processor)	SCCs flow-through under Art. 28(4); AWS DPA includes Module 3 SCCs	no	Same Schrems II posture. Encryption-at-rest with controller-held KMS keys mitigates.
US (Analytics Inc. sub-processor)	Pending sub-processor approval; SCCs flow-through under Art. 28(4)	no	Mitigation R-06 (drop sick-leave + remove sentiment scoring) reduces what crosses the boundary to this processor; final approval pending TIA addendum.

Processor compliance — Article 28

Processor	Country	DPA in place	Gap
PeopleFlow Inc.	US	yes	DPA covers Art. 28(3)(a-h) but Annex II TOMs need refresh to reflect supplementary technical measures from R-03 mitigation; sub-processor list to include analytics-pipeline vendor explicitly.
AWS (us-east-1)	US	yes	Flow-through via PeopleFlow's AWS contract; AWS DPA + Module 3 SCCs cover. Verify AWS region pinning to us-east-1 only — no copy-out.
Analytics Inc.	US	no	Sub-processor DPA not yet signed. Block go-live until DPA + SCCs flow-through executed and TIA addendum complete.

Article 36 prior-consultation determination

Consultation required: False

After mitigation, no residual risk scores at or above 9 on the 1–16 scale and no residual band reaches 'maximum'. Highest residual is R-02 (discriminatory profiling) at 6 — controllable via the documented Art. 22 safeguards. Mitigation completion is the precondition. Pre-mitigation, R-06 (sick-leave feature) and R-10 (DE works-council) would have triggered Article 36. Mitigation R-06 is a hard pre-requisite — if not implemented, the workflow recommends prior consultation.

Residual high risks:

- **R-02** (score after: 6) — Bias-mitigation effectiveness only verifiable post-deployment via the published fairness audit; controller commits to quarterly re-audit and an Art. 22 human-review override.
- **R-03** (score after: 6) — Schrems II posture cannot be reduced below 6 through controller-side measures alone; reliant on DPF stability + supplementary technical measures.