GSTRIDE AI

HYBRID WORK POLICY TEMPLATE · 2026 EDITION

Hybrid Work Policy Template.

A ready-to-customise hybrid work policy covering EU AI Act, GDPR, and the Digital Personal Data Protection Act 2023 in one document. 8 sections, three-region notes (EU / India / US), and drop-in appendix text. Built for HR Heads, COOs, and People Ops rolling out productivity intelligence across a cross-region workforce.

FOR
[Company Name]

OWNER
[Head of People / DPO]

EDITION
v1.0 · May 2026

Disclaimer. This template is a policy-drafting aid, not legal advice. The EU AI Act enters phased application through 2026 with implementing acts still to land; the Digital Personal Data Protection Act 2023 is in force with DPDP Rules expected late 2025 / 2026; US state laws (CPRA, NY S2628, CT 31-48d, DE 19 Del.C. § 705, NYC Local Law 144) continue to evolve — verify the latest position with counsel before any compliance assertion. Penalty exposure under the EU AI Act can run up to EUR 35 million or 7 percent of worldwide annual turnover for prohibited-AI infringements, subject to revision; DPDP penalties run up to INR 250 crore per category in the headline tier, also subject to revision under final Rules — verify with counsel before quoting. gStride is not certified by any data protection authority, the Data Protection Board, the Ministry of Electronics and Information Technology, or the European AI Office; this template describes architecture and operating choices, not regulatory endorsement.

How to use this template

This is an **8-section hybrid work policy template** built for an HR Head, COO, or People Ops lead rolling out a productivity intelligence platform across an EU + India + US workforce. It is built to be customised — every section carries explicit bracketed values where your company's name, contacts, and dates drop in, and every section carries region-specific notes for the three jurisdictions the template covers.

The 8 sections sit at the policy level. Read together, they cover scope, notice and consent, the monitoring boundary, AI usage, employee rights, retention, audit cadence, and exception handling. Two appendices follow with drop-in notice text for each region and a policy register table.

SECTION 1

Scope & Applicability. Who, where, and what the policy covers.

SECTION 2

Notice & Consent. What employees are told and how consent is recorded.

SECTION 3

Monitoring Boundaries. Signals collected and explicitly not collected.

SECTION 4

AI Usage & Inference. What AI can drive and the human-oversight rules.

SECTION 5

Employee Rights & Self-Service. Access, correction, erasure, portability, objection.

SECTION 6

Retention & Deletion. How long each data category is held.

SECTION 7

Audit & Review Cadence. Annual review and out-of-cycle triggers.

SECTION 8

Exception Handling & Escalation. Investigations, grievance, regulator, breach.

How the region notes work. Each section closes with three tagged notes — EU, India, US — pointing to the specific statute, regulator, or risk that applies in that jurisdiction. Treat them as drafting prompts: keep them in the policy if the section is in your scope, strip them out if your workforce is single-region, and always verify the cited statute with counsel before publication.

Recommended customisation workflow. One pass with the Head of People to fill bracketed values; second pass with the Data Protection Officer or equivalent for Sections 2, 4, 6, and Appendix A; third pass with the General Counsel for the lawful-basis assertions and penalty references. Send to the works council or Betriebsrat where applicable. Set the next review date in Appendix B and load the open actions into the People Ops register.

SECTION 1

Scope & Applicability

Intent. *Define which employees, contractors, locations, and working patterns this policy covers — and where it does not apply.*

This policy applies to all **[Company Name]** employees, fixed-term staff, and consultants who work in a hybrid pattern — meaning any combination of office, home, co-working, or third-location working across a regular working week. It covers desktop, laptop, and mobile-device work performed in connection with the employment relationship.

For employees based in the European Union or European Economic Area, this policy is read together with the GDPR notice in *[link to GDPR Article 13/14 notice]*. For employees in India, this policy is read together with the DPDP Act 2023 notice in *[link to DPDP Section 5 notice]*. For US-based employees, applicable state law (including but not limited to California CPRA, New York NYCAA, Connecticut, and Delaware monitoring statutes) is respected through the addenda in Appendix A.

It does not apply to: (a) work performed under client-issued devices governed by a separate client-vendor policy; (b) activity outside the working day on personal devices not connected to corporate systems; (c) processing of personal data that is not connected to the employment relationship.

REGION NOTES

- **EU** — Cross-reference works council consultation rights under EU directive 2002/14/EC where applicable. In Germany, the Betriebsrat must be consulted before adopting this policy.
- **INDIA** — For Indian employees, "data principal" in DPDP usage refers to the employee. Consent must be obtained in a language the employee understands — translations into regional languages on request.
- **US** — Some US states (CT, DE, NY) require advance written notice to employees before any electronic monitoring begins. See Appendix A for state-specific notice text.

SECTION 2

Notice & Consent

Intent. *Set out what the company tells employees about productivity intelligence processing, when consent is sought, and how it can be withdrawn.*

[Company Name] processes a defined set of work-context signals to maintain a productive, accountable, and fair working environment. Before any processing begins, every employee receives: (1) a plain-language notice describing what signals are collected, why, how long they are kept, who can access them, and what rights the employee holds; (2) where consent is the lawful basis, a granular consent form covering each processing purpose separately — not a single bundled tickbox.

Consent (where it is the lawful basis) is recorded against the employee record with timestamp, scope, and purpose. Consent can be withdrawn at any time through the employee self-service dashboard. Withdrawing consent does not trigger a hidden audit flag, manager notification, or any impact on the employee's performance record. Where the lawful basis is legitimate interest (EU) or legitimate use (India), employees retain the right to object, and the company will weigh the objection against a documented balancing test.

Notice is refreshed: (a) at hire; (b) on any change to the signals processed; (c) annually as part of the policy review cycle.

REGION NOTES

- **EU** Under GDPR, consent in an employment context is rarely a valid lawful basis due to the power imbalance. Default to legitimate interest with a documented balancing test, except for any processing that requires explicit consent (e.g., biometric data).
- **INDIA** DPDP Section 4 requires consent that is free, specific, informed, unconditional, and unambiguous. Bundled tickboxes are non-compliant.
- **US** CPRA and similar state laws require a "notice at collection" before or at the point any personal data is collected. The notice must list categories, purposes, retention, and the rights available.

SECTION 3

Monitoring Boundaries — What Is and Is Not Collected

Intent. *List by name every signal collected, every signal explicitly not collected, and the boundary between work-context and personal-life data.*

[Company Name] collects the following work-context signals only: (a) application and document focus time during the working day on corporate-issued devices; (b) commit cadence and other tool-level work artefacts on systems the employee uses for work; (c) calendar and meeting metadata where shared with the company; (d) self-reported flow-state and focus markers from the productivity dashboard.

The following are explicitly **not** collected under this policy: (i) screenshots of the employee's screen; (ii) keystroke logging; (iii) continuous webcam or microphone capture; (iv) any signal outside the working day on a personal device; (v) any content of personal communication, social media, or non-work documents; (vi) any biometric data unless separately consented to under a distinct biometric policy.

Any future addition to the collected signal set requires: (a) prior Data Protection Officer or equivalent sign-off; (b) policy version bump with employee notice; (c) updated lawful-basis assessment.

REGION NOTES

EU Default-on screen capture or keystroke logging is incompatible with GDPR proportionality and is recognised as a high-risk AI system under the EU AI Act (subject to revision under final implementing acts).

INDIA Under DPDP Section 4-5, surveillance defaults inverted to ON would render any consent collected after install non-compliant — the data subject has already been captured before the notice was read.

US State monitoring statutes (CT, DE, NY) do not prohibit keystroke logging but require written notice before any monitoring begins. The company's position is to not collect these signals regardless of state-level permissibility.

SECTION 4

AI Usage & Inference

Intent. *Describe how AI inference is applied to the collected signals, what decisions it can and cannot drive, and the human-oversight rules.*

[Company Name] uses AI inference to produce productivity signals — focus depth, commit cadence, flow-state minutes, meeting load, blocker recovery — to help employees and managers identify patterns over rolling windows. AI inference is a decision-support input. It is **not** the sole basis of any decision that has legal or similarly significant effect on an employee.

The following decisions are out of scope for AI inference and require documented human review with the inference signal as one of several inputs: (a) hiring; (b) compensation; (c) promotion or demotion; (d) performance improvement plans; (e) termination; (f) disciplinary action. AI inference may surface a pattern (e.g., declining focus depth over four weeks) — the decision on action remains with the human manager and HR business partner.

Every AI inference is logged with: model version, input signal categories, output, and the human decision (if any) taken in response. Logs are retained per the retention schedule in Section 6 and made available to the employee on request.

REGION NOTES

EU EU AI Act treats AI systems used in employment for performance evaluation, task allocation, and termination as high-risk (subject to revision under final implementing acts). High-risk systems require risk management, data governance, transparency, human oversight, accuracy, and post-market monitoring.

INDIA DPDP does not yet have AI-specific provisions; the Digital India Act draft is expected to introduce them. Until then, AI-driven decisions on employees should be assessed under DPDP Section 8 risk-management obligations.

US NYC Local Law 144 requires bias audits for automated employment decision tools; Illinois, Colorado, and California have related disclosure requirements. Where the tool drives hiring or promotion, the bias audit obligation applies.

SECTION 5

Employee Rights & Self-Service

Intent. *List the rights every employee holds over their data and the self-service workflows the company provides to exercise them.*

Every employee covered by this policy holds the following rights: (a) **access** — to see all data held about them; (b) **rectification** — to correct inaccurate data; (c) **erasure** — to request deletion subject to lawful retention obligations; (d) **portability** — to receive data in a machine-readable format; (e) **objection** — to object to processing based on legitimate interest; (f) **restriction** — to limit processing in defined circumstances; (g) **withdraw consent** — where consent is the basis.

Rights are exercised through the employee self-service dashboard at *[link]*. Response service levels: 30 days (EU/UK GDPR), inside the statutory window once notified (India DPDP), 45 days (California CPRA). The employee receives written acknowledgement within 5 working days and a substantive response within the applicable statutory window.

Where a right is refused (e.g., erasure conflicts with a tax-records retention obligation), the company provides written reasons and the employee's onward escalation path (Data Protection Officer, supervisory authority).

REGION NOTES

- **EU** — GDPR Articles 15-22 grant the listed rights. Article 22 prohibits decisions based solely on automated processing producing legal or similarly significant effects, subject to narrow exceptions.
- **INDIA** — DPDP Sections 11-14 grant access, correction, erasure, and nomination rights. The nominee is uniquely an Indian statutory right and must be supported in the self-service dashboard.
- **US** — CPRA, CDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), UCPA (Utah) grant similar rights. Apply the most protective standard where multiple state laws apply to one workforce.

SECTION 6

Retention & Deletion

Intent. *State how long each category of data is held and when it is deleted — both the routine schedule and the exception triggers.*

Productivity intelligence signals are retained per the schedule below. After the retention period ends, data is automatically deleted from production systems and from any analytics warehouse. Backup copies follow a separate retention schedule that expires on the next backup rotation.

Standard retention. Application focus time and commit cadence: 13 months rolling. Calendar metadata: 13 months. AI inference outputs: 13 months. Self-reported flow-state markers: 13 months. Manager-driven productivity reviews and the AI inference signals that fed them: 24 months (so they cover one full performance review cycle plus one).

Exception triggers. Data may be retained longer if: (a) a legal or regulatory hold is in place; (b) an internal investigation or grievance is active; (c) the employee has consented to extended retention for a specific purpose. The longer retention requires a documented reason and is reviewed quarterly.

REGION NOTES

- **EU** GDPR Article 5(1)(e) storage limitation requires retention proportionate to purpose. 13 months balances trend visibility against minimisation.
- **INDIA** DPDP Section 8 obliges the data fiduciary to delete personal data when the purpose has been served, subject to specific retention obligations under other laws.
- **US** CPRA requires disclosure of retention periods; state-specific employment record retention laws (often 3-7 years) take precedence where they apply.

SECTION 7

Audit & Review Cadence

Intent. *Set out who reviews this policy, how often, what triggers an out-of-cycle review, and the audit trail that proves it.*

This policy is reviewed at least **annually** by the named owner (see Appendix B) with sign-off from the Data Protection Officer or equivalent, the Head of People, and the General Counsel. The annual review covers: lawful basis assessment, signal-set audit, inference-model audit (bias and drift), retention compliance, rights-request volume and SLA performance, incident retrospectives, and regulatory horizon scan.

Out-of-cycle triggers requiring an immediate review include: (a) any addition to the signal set; (b) any new AI inference model deployed; (c) any notified regulatory change (EU AI Act implementing acts, DPDP Rules notification, US state legislation); (d) any data breach involving productivity signals; (e) any successful objection or rights request that exposes a policy gap.

Each review produces a dated, signed minute that is retained in the policy register. The minute includes: scope reviewed, findings, actions opened, action owners, and target close dates. Open actions are tracked monthly in the People Ops operations review.

REGION NOTES

- **EU** — EU AI Act high-risk systems require post-market monitoring (subject to revision); the annual review satisfies this for the employment-AI use case where it is appropriately scoped.
- **INDIA** — DPDP Section 10 imposes periodic audit obligations on Significant Data Fiduciaries; the annual review meets the indicative cadence ahead of Rules notification.
- **US** — NYC Local Law 144 bias audits are required annually for AEDT tools; the cadence here is aligned.

SECTION 8

Exception Handling & Escalation

Intent. *Define what happens when this policy collides with operational reality — investigations, grievances, regulator requests, breach response.*

Investigations. If a documented investigation requires processing outside the normal signal scope (e.g., reviewing communication content in a misconduct case), the investigation lead must obtain written authorisation from the Data Protection Officer and the General Counsel. The authorisation specifies scope, purpose, retention, and the employee notice path. Investigation-driven processing is logged in the policy register.

Employee grievance. An employee who believes this policy has been breached may raise a grievance through the standard grievance procedure or directly to the Data Protection Officer at *[dpo@company]*. The DPO acknowledges within 5 working days and substantively responds within 30 days. The employee retains the right to escalate to the relevant supervisory authority (data protection authority, equal opportunity commission, labour court).

Regulator request. Requests from data protection authorities, labour inspectorates, or other regulators are routed to the General Counsel within 24 hours. The company responds within the statutory window with a documented and minuted response.

Breach response. Any breach affecting productivity-intelligence data is handled per the company's incident response runbook. Notification timelines: 72 hours to the supervisory authority (EU GDPR), inside the statutory window once notified (India DPDP), per the applicable US state breach-notification law. Affected employees are notified without undue delay where the breach is likely to result in high risk.

REGION NOTES

- **EU** GDPR Article 33 (72-hour authority notification) and Article 34 (data-subject notification where high-risk) apply.
- **INDIA** DPDP Rules drafts indicate a notification expectation to the Data Protection Board; verify exact timeline with counsel once Rules are notified.
- **US** State breach notification laws vary by state. Apply the most protective standard where multiple state laws apply.

Appendix A — Region-specific notice text

Drop-in notice paragraphs for the three jurisdictions covered by this template. Customise the bracketed values, drop into your employee handbook, and have counsel verify before publication.

EU / EEA — GDPR Article 13/14 notice

This notice describes how **[Company Name]**, the data controller, processes your personal data in connection with our hybrid working policy. Our lawful basis is **[legitimate interest / explicit consent]**. We process the categories listed in Section 3 for the purposes described in this policy. Your rights and the path to exercise them are set out in Section 5. Contact: *[dpo@company]*.

India — DPDP Section 5 notice

This notice tells you, the data principal, how **[Company Name]**, the data fiduciary, processes your personal data. We process the categories in Section 3 for the purposes in this policy. You may withdraw consent, exercise access, correction, erasure, and nomination rights, and lodge a complaint with the Data Protection Board. Contact: *[dpo@company]*. Translation into *[regional language]* is available on request.

US — State monitoring notice

This notice is provided in advance of any electronic monitoring under **[Company Name]**'s hybrid working policy. It describes the categories of work-context activity that may be monitored, the purpose, and your rights under applicable state law (CPRA / NY S2628 / CT 31-48d / DE 19 Del.C. § 705 / similar). Your rights and the path to exercise them are in Section 5. Contact: *[privacy@company]*.

Appendix B — Policy register and owner table

FIELD	VALUE
Policy owner	[Head of People]
DPO / equivalent	[Data Protection Officer]
Approver — Legal	[General Counsel]
Approver — Security	[CISO]
Version	v1.0
Effective date	[YYYY-MM-DD]
Next scheduled review	[YYYY-MM-DD] (annual)
Works council / Betriebsrat consultation	[Date / N/A]

Want a second pair of eyes on the customisation?

If you are about to publish this policy across an EU + India + US workforce and want an independent read on the lawful-basis assessment, retention schedule, or signal set before rollout, book a 30-minute readiness audit with the gStride team. We will walk through your draft, flag the regional gaps that matter most, and share the deployer-side templates we ship to our own customers.

Book a 30-min readiness audit · cal.com/gstrideai/30min

Interactive online preview at **gstride.ai/assets/audits/hybrid-work-policy-template.html** — tick your region (EU / India / US / Global) and company size band to see customised section excerpts.