DATA PRIVACY BHARAT CENTER (DPBC)

A Unit of KETAS Education Foundation & World Cyber Security Forum

(Registered as a Non-Profit Organisation under Section 8 with 12A and 80G)

www.ketasedufoundation.org/data-privacy-bharat-centre

Date: 26th April 2026

To,
The Secretary
Ministry of Electronics and Information Technology (MeitY)
Government of India
Electronics Niketan, 6, CGO Complex
New Delhi – 110003

Subject: *A Citizen-Centric Policy Brief on Strengthening the Guidelines for Indian Government Websites and Apps (GiGW 3.0) considering the Digital Personal Data Protection Act, 2023*

Respected Sir/Madam,

We write on behalf of the **Data Privacy Bharat Center (DPBC),** a unit of **KETAS Education Foundation** *(a not-for-profit organization) (S.8 company with 80G & 12A certified),* working in the public interest at the intersection of digital governance, data protection, and citizen rights. Our work is grounded in the principle that India's leadership in digital public infrastructure must be matched by equally strong standards for transparency, accessibility, and accountability across every government-facing digital service.

This submission consolidates the findings of a four-part study undertaken by our team. It examines four elements:

(a) The interplay between GiGW 3.0 and the Digital Personal Data Protection Act, 2023; (b) Field observations from leading central government portals;

(c) A comparative analysis of GiGW 3.0 against global digital-governance frameworks in the European Union, the United Kingdom, the United States, and Singapore; and

(d) 10 policy recommendations grouped under five reform themes. A sample citizen-friendly privacy notice template is appended as an annexure for ready reference.

The recommendations are offered in a constructive spirit, with the intent of strengthening — not replacing — the foundation laid by GiGW 3.0.

We would be glad to support MeitY through further consultations, working-group participation, or implementation pilots, as may be useful and can be reached out on the provided contact number and email address for any discussions.

With sincere regards,

Prof (Dr.) Nachiketa Mittal
Founder, KETAS Education Foundation
Curator, Data Privacy Bharat Center (DPBC)
+91 78734 75690
mittal.keta@gmail.com
www.ketasedufoundation.org/data-privacy-bharat-centre

Executive Summary

The Guidelines for Indian Government Websites and Apps (GiGW 3.0) have played a foundational role in standardising the design, accessibility, and security of government digital platforms. Three converging shifts, however, have surfaced gaps that GiGW in its current form does not adequately address: the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act); the maturation of global digital-government frameworks; and rising citizen expectations of digital services.

Methodology

This policy brief draws on three strands of research:

- **A DPDP-aligned gap analysis** of GiGW, identifying where its provisions intersect with — and fall short of — the personal-data obligations established by the DPDP Act, 2023.
- **Field observations** from a review of leading central government portals, drawing out illustrative gaps in privacy disclosure, accessibility transparency, security trust signals, and citizen feedback mechanisms.
- **A comparative analysis** of GiGW 3.0 against the EU Web Accessibility Directive, the UK Government Digital Service Standard, the US Digital Services Playbook, and the Singapore Government Digital Service Standards.

Headline Findings

- GiGW mandates the presence of a privacy policy but does not specify the form, depth, or DPDP-aligned content of that notice.
- Government portals carry cookie disclosures but provide no consent banner or user-control interface, falling short of the DPDP affirmative-consent standard.
- Accessibility features exist on most major portals, but public accessibility statements and independent audit reports — required under the EU Web Accessibility Directive — are absent in India.

- Security practices are robust at the backend but are not visibly communicated to citizens through trust signals or vulnerability disclosure channels.
- Service-level feedback and grievance mechanisms are not consistently embedded in citizen journeys, in contrast to UK and Singapore practice.

Headline Recommendations

Based on the above, the brief proposes ten policy recommendations under five reform themes. Each recommendation is set out in detail in Part IV.

#	Reform Theme	Recommendation (in brief)
1	Privacy & Data Governance	Mandate dataset-level privacy notices aligned with the DPDP Act
		Require cookie and tracker consent management with affirmative opt-in
2	Accessibility & Inclusion	Mandate public accessibility statements and annual third-party audits
		Establish a National Government Design System with multilingual templates
3	Security & Digital Trust	Require visible security trust signals and a Vulnerability Disclosure Policy
		Mandate Data Protection Impact Assessments for high-risk integrations
4	Citizen-Centric Service Delivery	Embed service-level feedback and grievance mechanisms
		Adopt phased service development with mandatory user research
5	Compliance Monitoring	Launch a public GiGW Compliance Dashboard
		Issue a joint GiGW–DPDP compliance framework

Part I — Why GiGW Needs Strengthening: A DPDP Act Perspective

GiGW 3.0 aims to standardise quality, accessibility, cybersecurity, and lifecycle management across government digital platforms. The Digital Personal Data Protection Act, 2023 (DPDP Act), in parallel, establishes a framework for the lawful, transparent, and accountable processing of citizens' personal data. This Part examines how the two frameworks intersect, identifies key gaps from a DPDP perspective, and sets out the implications for policy reform.

1.1 How GiGW Triggers the Processing of Personal Data

In pursuit of its quality, accessibility, cybersecurity, and lifecycle goals, GiGW directs government websites, web portals, and mobile applications to operate features and infrastructure that collect, store, or transmit personal data. The table below sets out an illustrative — though not exhaustive — list of GiGW-aligned design and operational practices that constitute personal-data processing under the DPDP Act.

GiGW Trigger Area	Nature of Personal Data Processing
Feedback and newsletters	Collection of visitor names, email addresses, phone numbers, and free-text feedback (which may itself contain personal data).
Authentication and identity integrations	Exchange and processing of identity data and supporting documents (personal and sensitive identifiers, including Aadhaar-linked data).
Credentials and session management	Storage and handling of authentication credentials and session tokens that, in turn, enable access to personal data.

GiGW Trigger Area	Nature of Personal Data Processing
Databases and backups	Centralised storage, backups, and off-site copies of personal data — all of which qualify as processing under the DPDP Act.
Logging and monitoring	Retention of logs containing IP addresses, access records, and behavioural data.
Third-party and social integrations	Sharing of user content and identifiers with external platforms; possibility of cross-border data transfers.
OCR and digitisation of scanned documents	Conversion of scanned documents into machine-readable personal data for storage and downstream processing.
Analytics and engagement monitoring	Collection of behavioural data, email lists, and profiling for engagement and outreach.

1.2 Key Gaps between GiGW and the DPDP Act

The DPDP Act establishes specific obligations for every entity that processes personal data — including government departments. GiGW, in its current form, does not yet operationalise these obligations. The table below sets out the principal gaps.

DPDP Act Requirement	GiGW Position	Policy Issue	Citizen Impact
Clear purpose, lawful basis, and data minimisation	No requirement of consent banners or principles of data minimisation	Citizens are not clearly informed, at a granular level, about what data is collected and why.	Limited visibility into how and why their personal data is used.

DPDP Act Requirement	GiGW Position	Policy Issue	Citizen Impact
Affirmative, purpose-specific consent and easy withdrawal	No mandatory consent UX for cookies, analytics, newsletters, or integrations	Optional processing relies on bundled or implied consent, which does not meet the requirement of affirmative action.	Reduced ability of citizens to give or withdraw consent meaningfully.
Mandatory user rights (access, correction, erasure, nomination, revocation of consent)	No requirement to design mechanisms for users to exercise these rights	Access, correction, and erasure rights are not mandated through clear procedures or timelines, depriving citizens of an effective means to exercise these rights.	Difficulty or inability in exercising rights such as access, correction, or erasure.
Retention periods to be specified and linked to purpose	Fixed log retention permitted, without dataset-level justification	Long-term data retention compromises the consent of data principals by retaining data for longer than the purpose for which it was given.	Increased exposure from prolonged retention of logs and digitised records.

DPDP Act Requirement	GiGW Position	Policy Issue	Citizen Impact
Processing by data processors to be informed and backed by contracts	No requirement for Data Processing Agreements; current privacy policy templates are not sufficient to inform users about third-party processors	Citizen data is shared with third-party processors without necessary safeguards, expanding the scope of use beyond what consent permits.	Citizens' data is exposed to risk of misuse on account of an absence of contractual safeguards.

1.3 Implications for Policy Reform

To align GiGW with the DPDP Act and strengthen citizen trust, the following directions emerge from the analysis above:

- Introduce dataset- and feature-level privacy notices, consent banners, and clear purpose mapping at the point of data collection.
- Mandate consent-management mechanisms for all optional processing, with granular opt-in and easy withdrawal.
- Require Data Protection Impact Assessments (DPIAs) or equivalent assessments for high-risk integrations such as biometric authentication, payments, and large-scale analytics.
- Operationalise user rights — access, correction, erasure, withdrawal — through clear procedures, timelines, and audit trails.
- Ensure transparency and contractual safeguards for all third-party data processors, including standardised Data Processing Agreements.

Part II — Evidence from the Field: Observations from Central Government Portals

The gaps identified in Part I are not theoretical. This Part documents observations from a review of four central government websites, selected to span the four reform areas highlighted earlier — privacy, accessibility, security and trust, and citizen experience. The websites reviewed are well-administered and publicly accessible. The observations point not to failures of any department, but to structural gaps in the GiGW framework itself.

2.1 Privacy

Case 1 — Central Information Commission

Website: *cic.gov.in* **|** **Type:** Central

Observed Issue: The privacy policy is generic and lacks details on data retention periods, user rights, or data deletion mechanisms.

Underlying GiGW Gap: GiGW mandates the presence of a privacy policy but does not enforce a standardised, detailed privacy-notice format aligned with data-protection laws.

Citizen Impact: Users cannot clearly understand how their personal data is collected, used, or retained.

2.2 Accessibility

Case 2 — Unique Identification Authority of India

Website: *uidai.gov.in* **|** **Type:** Central

Observed Issue: Accessibility features exist on the portal, but no publicly available accessibility statement or compliance report is provided.

Underlying GiGW Gap: GiGW recommends WCAG conformance but does not require mandatory accessibility statements, third-party audits, or public reporting.

Citizen Impact: Persons with disabilities may face barriers, with no clarity on the accessibility support available or the redress channels open to them.

2.3 Security and Trust

Case 3 — Reserve Bank of India

Website: *rbi.org.in* | **Type:** Central

Observed Issue: There is limited visibility of security-assurance measures such as published certifications or vulnerability disclosure policies.

Underlying GiGW Gap: GiGW focuses on backend cybersecurity practices but lacks provisions for displaying user-facing security trust indicators or transparency mechanisms.

Citizen Impact: Users may be uncertain about the authenticity and security posture of the digital services they rely upon.

2.4 Citizen Experience

Case 4 — Digital India Programme

Website: *digitalindia.gov.in* | **Type:** Central Portal

Observed Issue: There is limited integration of feedback or grievance mechanisms within service-level or informational pages.

Underlying GiGW Gap: GiGW does not mandate embedded, service-level feedback and grievance mechanisms.

Citizen Impact: Citizens may find it difficult to report issues or seek clarifications efficiently.

2.5 Patterns Across the Cases

Five recurring patterns emerge from the observations above:

- Privacy policies are present but lack depth, standardisation, and clarity on user rights.
- Cookie disclosures exist, but consent mechanisms are largely absent.
- Accessibility compliance is inconsistent and unaccompanied by public reporting.
- Security practices are implemented but not visibly communicated to users.
- Feedback and grievance systems are not integrated into user journeys.

Part III — Global Benchmarking: How India Compares

While the patterns identified in Part II point to specific deficits within India's framework, comparable governments abroad have addressed many of these challenges through dedicated standards. This Part sets out a comparative analysis of GiGW 3.0 against six leading international frameworks: the European Union's General Data Protection Regulation (GDPR) and Web Accessibility Directive; the United Kingdom's Government Digital Service Standard; the United States Digital Services Playbook; and Singapore's Government Digital Service Standards. Although these frameworks vary in scope and legal character, their combined practice illuminates the directions in which mature digital-government regimes are evolving.

3.1 Key Differences in Regulatory Character

Scope and Regulatory Nature

- **GiGW 3.0** is a technical guideline focused on the design, accessibility, security, and lifecycle management of government websites and applications.
- **GDPR (EU) and the DPDP Act (India)** are data-protection laws that regulate the lawful processing of personal data and establish enforceable user rights.
- **EU Web Accessibility Directive** focuses specifically on accessibility compliance, including mandatory public accessibility statements.
- **UK, US, and Singapore digital service standards** address the end-to-end design, delivery, and governance of citizen digital services.

Privacy and Data Governance

GDPR and the DPDP Act emphasise data minimisation, affirmative consent, the right to access and erase data, and breach notification. GiGW 3.0, by contrast, focuses primarily on backend security practices and safe hosting, rather than on user data rights.

Accessibility Enforcement

The EU Web Accessibility Directive mandates accessibility statements, citizen feedback mechanisms, and periodic monitoring and reporting. GiGW includes WCAG conformance recommendations but lacks formal public accessibility reporting requirements.

Service Design Philosophy

The UK, US, and Singapore frameworks adopt user-centric service design as a core principle. Singapore's Digital Service Standards, in particular, emphasise usability, performance, and citizen-centric digital experiences. GiGW includes UI/UX guidance but does not fully institutionalise structured service-design processes.

Performance and Service Monitoring

Mature frameworks emphasise continuous performance monitoring backed by analytics and citizen feedback. GiGW includes monitoring dashboards but focuses largely on compliance monitoring rather than citizen-experience metrics.

3.2 Comparative Matrix

The matrix on the following page sets out a side-by-side comparison of GiGW 3.0 against the principal global frameworks, across fifteen governance dimensions. The matrix is presented in landscape orientation for legibility.

Comparative Matrix: GiGW 3.0 vs Global Digital Governance Standards

Governance Dimension	GiGW 3.0 (India)	GDPR (EU)	DPDP Act (India)	EU Web Accessibility Dir.	UK Digital Service Standard	US Digital Services Playbook	Singapore Digital Svc. Standards
Type of Framework	Government website & app guidelines	Data protection regulation	Data privacy law	Accessibility regulation	Digital service delivery standard	Digital service design playbook	Government digital service standards
Primary Objective	Standardise government websites & apps	Protect personal data and privacy	Regulate personal data processing	Ensure accessibility for public-sector websites/apps	Deliver user-centred public services	Improve federal digital services	Deliver high-quality citizen digital services
Legal Enforceability	Mandatory for government portals	Legally binding with penalties	Legally binding	Legally binding	Mandatory for UK government services	Policy guidance	Mandatory for Singapore government services
Coverage Scope	Government websites & mobile apps	All organisations processing EU data	Data fiduciaries handling personal data	Public-sector digital services	All UK government digital services	US federal digital services	Singapore government digital services

Governance Dimension	GiGW 3.0 (India)	GDPR (EU)	DPDP Act (India)	EU Web Accessibility Dir.	UK Digital Service Standard	US Digital Services Playbook	Singapore Digital Svc. Standards
Accessibility Compliance	WCAG 2.1 Level AA recommended	Limited	Limited	WCAG 2.1 Level AA mandatory	Strong accessibility requirements	Strong accessibility requirements	Strong accessibility requirements
Privacy & Data Protection	Limited focus	Comprehensive data protection	Core focus	Limited	Moderate	Moderate	Moderate
User-Centric Design	Partial guidance	Not primary focus	Not primary focus	Not primary focus	Core principle	Core principle	Core principle
Security Requirements	Strong (cybersecurity guidelines)	Strong (data security obligations)	Strong	Moderate	Moderate	Moderate	Strong
Service Lifecycle Management	Website lifecycle & governance	Not applicable	Not applicable	Not applicable	Full-service lifecycle approach	Service lifecycle approach	Full lifecycle governance
Performance Monitoring	Compliance dashboards	Not applicable	Not applicable	Limited	Continuous performance monitoring	Analytics-driven improvement	Performance monitoring dashboards

Governance Dimension	GiGW 3.0 (India)	GDPR (EU)	DPDP Act (India)	EU Web Accessibility Dir.	UK Digital Service Standard	US Digital Services Playbook	Singapore Digital Svc. Standards
Accessibility Reporting	Limited	No	No	Mandatory accessibility statements & audits	Required	Encouraged	Required
Govt. Digital Infra. Integration	Strong (Aadhaar, DigiLocker, SSO)	Not applicable	Limited	No	Moderate	Moderate	Strong national platforms
Design System / UI Standardisation	Basic UI guidelines	Not applicable	Not applicable	Limited	GOV.UK Design System	US Web Design System	Singapore Government Design System
Citizen Feedback Mechanisms	Basic feedback channels	Data-subject rights	Grievance redressal	Feedback mechanisms	Strong user feedback integration	User testing and feedback loops	Citizen feedback integrated
AI / Emerging Tech Governance	Limited	Emerging provisions	Limited	No	Emerging	Emerging	Increasing focus

3.3 International Best Practices India Could Adopt

Distilling the comparative analysis above, six clusters of best practice emerge as particularly relevant for the next iteration of GiGW:

Best-Practice Theme	Reference Framework	Components
Stronger Privacy-by-Design	GDPR / DPDP Act	Privacy by design • Explicit consent management • Data minimisation • Breach reporting requirements
Mandatory Accessibility Reporting	EU Web Accessibility Directive	Accessibility statements for every government site • Public feedback mechanism • Periodic compliance audits • Transparency reports
User-Centric Service Design	UK Digital Service Standard	Mandatory user research before service launch • Service prototypes and usability testing • Multidisciplinary delivery teams
Continuous Service Monitoring	US Digital Services Playbook	Service performance dashboards • Analytics-based service improvement • User satisfaction metrics
Unified Government Design System	Singapore Digital Service Standards	National Government Design System • Reusable UI components • Unified accessibility templates • Multilingual UI frameworks
Digital Ethics and Responsible AI	Emerging global practice	AI governance • Algorithm transparency • Ethical data usage

Part IV — Ten Recommendations for Strengthening GiGW

Drawing together the gap analysis in Part I, the field observations in Part II, and the comparative analysis in Part III, this Part sets out ten policy recommendations grouped under five reform themes. Each recommendation follows a Problem → Proposed Solution → Expected Impact structure and is offered for MeitY's consideration as part of the next iteration of GiGW.

Theme 1: Privacy & Data Governance

Recommendation 1 — Mandate Dataset-Level Privacy Notices Aligned with the DPDP Act

Problem: GiGW requires the presence of a privacy policy but does not specify form or depth. As Case 1 (Central Information Commission) illustrates, reviewed portals carry generic notices that omit retention periods, user rights, and deletion mechanisms. This falls short of the DPDP Act's notice obligations, which require purpose-specific, plain-language disclosure at the point of collection.

Proposed Solution: MeitY to issue a standardised, layered privacy-notice template — applied at the dataset and feature level (forms, login flows, analytics, OCR pipelines, third-party integrations). Each notice should disclose: data collected, purpose, lawful basis, retention period, third-party recipients, user rights, and grievance contact.

Expected Impact: Citizens gain clear, granular visibility into how their data is processed; government departments achieve baseline DPDP-readiness; legal exposure is reduced.

Recommendation 2 — Mandatory Cookie and Tracker Consent Management

Problem: As Case 2 (Department of Expenditure) illustrates, government websites frequently mention cookie usage but provide no consent banner or user-

control interface. Bundled or implied consent does not meet the DPDP Act's standard of free, informed, specific, and affirmative consent.

Proposed Solution: Require every government website to implement a standards-compliant consent banner with (a) granular opt-in toggles for non-essential cookies and trackers, (b) one-click withdrawal, (c) a tamper-evident consent log, and (d) a default state of "no tracking" until consent is given.

Expected Impact: Genuine user agency over tracking; alignment with DPDP affirmative-consent provisions; demonstrable accountability through audit trails.

Theme 2: Accessibility & Inclusion

Recommendation 3 — Mandatory Accessibility Statements and Annual Public Audits

Problem: GiGW recommends WCAG 2.1 Level AA conformance but does not require public accessibility statements or independent audit reporting. As Case 3 (UIDAI) illustrates, accessibility features are implemented without any public statement of conformance — a gap that the EU Web Accessibility Directive specifically addresses through mandatory statements and feedback mechanisms.

Proposed Solution: Every government website to publish a standardised accessibility statement covering scope, conformance level, known gaps, alternative-access channels, feedback contact, and redress timelines. Independent third-party audits to be conducted annually for high-traffic portals, with redacted reports published on a central dashboard.

Expected Impact: Transparent accountability for persons with disabilities; structured redress pathway; parity with global accessibility benchmarks.

Recommendation 4 — A National Government Design System for Multilingual and Inclusive Delivery

Problem: GiGW provides UI/UX guidance but does not institutionalise reusable, accessibility-first design components or multilingual delivery — leaving each department to build from scratch. Singapore's unified Government Design System demonstrates the productivity and consistency gains of this approach.

Proposed Solution: Establish a National Government Design System under MeitY/NIC, with reusable, accessibility-first components, multilingual templates, and clear language-coverage thresholds for high-impact citizen services (for example, a minimum of twelve scheduled languages for nationally-used portals).

Expected Impact: Reduced digital divide; faster, cheaper development cycles; a consistent citizen experience across portals.

Theme 3: Security & Digital Trust

Recommendation 5 — Visible Security Trust Signals and a Vulnerability Disclosure Policy

Problem: GiGW focuses on backend cybersecurity but offers little guidance on user-facing trust transparency. As Case 4 (Reserve Bank of India) illustrates, even mature portals display limited public information on security certifications or vulnerability reporting channels, leaving citizens unable to verify the trustworthiness of services.

Proposed Solution: Mandate a standardised "Security & Trust" page on every government portal, disclosing applicable certifications (CERT-In empanelment, ISO 27001 where relevant), date of last security audit, a published Vulnerability Disclosure Policy (VDP) with a dedicated reporting channel, and a breach-notification commitment aligned with the DPDP Act.

Expected Impact: Higher citizen confidence; a structured, lawful pathway for ethical security researchers; reduced effectiveness of phishing and look-alike portals.

Recommendation 6 — Data Protection Impact Assessments (DPIAs) for High-Risk Integrations

Problem: Government portals routinely integrate Aadhaar-based authentication, DigiLocker, payment gateways, OCR pipelines, and analytics platforms — all of which involve significant personal-data flows, as identified in Part I. GiGW currently mandates no risk-assessment process before such integrations go live.

Proposed Solution: Require a DPIA (or equivalent assessment) before deploying any portal that integrates biometric authentication, third-party SSO, payment processing, large-scale analytics, or cross-border data transfers. A DPIA summary to be filed with MeitY pre-launch, with a redacted version published.

Expected Impact: Risks surfaced and mitigated before deployment; practical alignment with DPDP obligations applicable to Significant Data Fiduciaries; stronger third-party governance.

Theme 4: Citizen-Centric Service Delivery

Recommendation 7 — Embed Service-Level Feedback and Grievance Mechanisms

Problem: As Case 5 (Digital India Programme) illustrates, major portals do not consistently integrate feedback or grievance channels at the service-page level. Citizens often must navigate away from a service to report issues — a friction the UK GOV.UK Service Standard specifically addresses through embedded feedback loops.

Proposed Solution: Mandate that every transactional or informational service page include (a) a lightweight "Was this helpful?" widget, (b) one-click access to a service-specific grievance channel with a published Service Level Agreement, and (c) feeds that flow into a department-level dashboard for continuous improvement.

Expected Impact: Faster issue resolution; richer signal for service teams; visible responsiveness that reinforces citizen trust.

Recommendation 8 — Phased Service Development with Mandatory User Research

Problem: GiGW offers UI/UX guidance but does not institutionalise discovery, alpha, beta, and live phases — phases that the UK GOV.UK Service Standard treats as mandatory gates. Services are often launched without structured user research, leading to low adoption and rework.

Proposed Solution: Adopt phased service-development gates for citizen-facing services above a defined scale, with mandatory user research at each phase.

Establish a Service Standard Assessment Panel within MeitY to review services before they progress through gates.

Expected Impact: Services that better fit citizen needs from launch; reduced rework costs; cultural shift toward user-centric delivery.

Theme 5: Compliance Monitoring

Recommendation 9 — A Public GiGW Compliance Dashboard

Problem: Compliance with GiGW is presently largely self-attested. Citizens have no way to view a portal's privacy-notice quality, accessibility audit status, security certifications, or grievance-response performance — making accountability diffuse.

Proposed Solution: Create a public "GiGW Compliance Dashboard" hosted on meity.gov.in, displaying portal-wise indicators: privacy-notice conformance, last accessibility audit, security certification status, content-update recency, and grievance SLA performance. Department-level scorecards updated quarterly.

Expected Impact: Accountability through transparency; healthy competitive pressure across departments; informed civil-society engagement.

Recommendation 10 — Converge GiGW with the DPDP Act through a Joint Compliance Framework

Problem: GiGW and the DPDP Act currently operate in parallel. As shown in Part I, government websites are simultaneously subject to GiGW design obligations and DPDP Act obligations as Data Fiduciaries — yet there is no unified compliance pathway, leading to duplication, ambiguity, and uneven implementation.

Proposed Solution: Issue a joint MeitY framework that (a) maps each GiGW clause to corresponding DPDP obligations, (b) designates every department's CIO (or a nominated officer) as the Data Protection Officer for its digital estate, and (c) embeds a standardised DPDP audit checklist within the existing GiGW assessment cycle.

Expected Impact: Reduced compliance overhead; legal certainty for departments; unified, coherent accountability for personal data and digital service quality.

Closing Submission

GiGW 3.0 represents a significant step forward in standardising government digital services in India. The recommendations set out in this brief are offered in a constructive spirit, with the intent of strengthening — not replacing — the existing framework. Adopting these measures would help ensure that the next iteration of GiGW reflects both India's constitutional commitments to its citizens and its emerging stature as a global leader in digital governance.

DPBC remains available to support MeitY through further consultations, working-group participation, or implementation pilots, as may be useful.

Contributors to this Brief

This brief has been prepared by a team at the Data Privacy Bharat Center (DPBC) comprising:

1. **Ms. Paakhhi Garg** (Policy Recommendations Lead & Editor)
2. **Mr. Ayush Sahay** (Policy Research Lead)
3. **Mr. Ashish Inamdar** (Government Website Case Study Lead)
4. **Mr. Anshuman Tripathi** (Global Best Practices Analyst)

— END OF MAIN BRIEF —

Annexure — Sample Citizen-Friendly Privacy Notice Template

A model template suitable for adaptation by any central or state government website, designed to comply with the DPDP Act, 2023 and to be readable by an ordinary citizen.

Privacy Notice — [Name of Department / Portal]

Last updated: [Date]

Available languages: [List]

1. What this notice tells you

This notice explains, in plain language, what personal data we collect from you when you use this website, why we collect it, how long we keep it, who we share it with, and the rights you have over your data.

2. Who is responsible for your data

Data Fiduciary: [Name of Department]

Data Protection Officer: [Name, Designation]

Contact: [Email] | [Phone] | [Postal address]

3. What data we collect and why

Data we collect	Why we collect it	Lawful basis	How long we keep it
Name, email, phone (when you submit a form / register)	To respond to your request and update you	Your consent	e.g., 2 years from last interaction
Login credentials (for registered services)	To authenticate you securely	Performance of public service	While account is active + 1 year

Data we collect	Why we collect it	Lawful basis	How long we keep it
IP address, device, browser logs	For security and to prevent misuse	Legitimate government function	e.g., 180 days
Cookies and analytics data (only with consent)	To improve the website	Your consent	e.g., 13 months
Documents you upload (e.g., scanned IDs)	For the specific service applied for	Your consent / statutory mandate	As required by relevant scheme

4. Who we share your data with

We share your data only with:

- Other government departments where required by law or to deliver the service you requested;
- Authorised technology service providers, who are bound by data-protection contracts;
- Law enforcement agencies, where legally required.

We do not sell your data. We do not share it for advertising.

5. Your rights under the DPDP Act, 2023

You have the right to:

- **Access** the personal data we hold about you;
- **Correct** any data that is inaccurate or incomplete;
- **Erase** your data when it is no longer needed for the purpose collected;
- **Withdraw consent** at any time, where consent is the basis of processing;
- **Nominate** another individual to exercise your rights in your absence;
- **File a grievance** if you believe your data has been mishandled.

To exercise any of these rights, please write to **[DPO email]**. We will respond within **[e.g., 30 days]**.

6. Cookies and tracking

This website uses cookies. **Essential cookies** (needed for the site to work) are always on. **Optional cookies** (analytics, preferences) are turned off by default and are used only if you accept them through our cookie banner. You can change your choice at any time from the "Cookie Preferences" link in the footer.

7. How we keep your data secure

We follow CERT-In guidelines and applicable Government of India information-security standards. Our last security audit was completed on **[date]**. To report a security vulnerability, please write to **[security@department.gov.in]** or visit our Vulnerability Disclosure Policy page.

8. If you have a complaint

If you are not satisfied with how we have handled your data:

- **Step 1:** Write to our Data Protection Officer at [DPO email].
- **Step 2:** If unresolved within 30 days, you may approach the Data Protection Board of India under the DPDP Act, 2023.

9. Changes to this notice

We will update this notice when our practices change. The "Last updated" date at the top will tell you when. Significant changes will also be highlighted on our home page for at least 30 days.

— END OF DOCUMENT —