# **Accenture Privacy Policy: Comprehensive Guide (Effective October 18, 2024)**

## **1. Overview & Scope**

Accenture’s privacy statement establishes high standards for protecting personal data across all its global services, websites, applications, digital tools, games, and data processing activities. The policy applies whenever Accenture acts as a "data controller"—meaning it is responsible for deciding how and why your personal data is used—with Accenture Global Holdings Limited representing non-EU data controllers in privacy matters.

The privacy statement is regularly updated to reflect changes in legal requirements and the company’s practices.

## **2. Data Protection Principles**

## **Commitment to Security**

Accenture commits to:

* Meeting all applicable legal and regulatory data protection requirements.
* Implementing appropriate technical, physical, and organizational measures to prevent unauthorized access, loss, alteration, or unlawful processing/destruction of personal data.
* Regularly auditing, testing, and enhancing security (ISO27001 certified, global client data protection program, regular penetration testing).

## **3. Categories of Personal Data Collected**

Accenture collects data in a wide variety of contexts, such as:

* Employees (current, former, prospective)
* Clients, suppliers, business partners, shareholders
* Website/app users and visitors

**Types of personal data collected:**

* **Personal details:** Name, contact details, gender (if needed), date/place of birth, identifiers
* **Commercial information:** Records of products/services, correspondence, transaction history
* **Marketing info:** IP address, social media handles, demographics, browsing data, preferences, analytics, speech-to-text requests
* **Sensitive data:** Health/medical info, biometrics, disability/access needs, dietary/allergy disclosures (for events), race/ethnicity, union membership, religious info (with consent/where legal)
* **Audiovisual data:** Photos, video/audio from CCTV, events, webinars, workshops, calls, meetings
* **Professional details:** Position, employer, job title, work location, system/application access ID
* **Recruitment info:** Education, career history, background checks, references, assessment results, salary info, immigration/data, diversity data
* **Cookies & geolocation data**
* **Cyber threat intelligence**: Data about digital threats to protect networks and data

**Sources:** Directly from individuals, affiliates, service providers, publicly available sources, recruitment firms, social media, clients, previous employers, public authorities.

## **4. Purposes for Processing Data & Legal Bases**

Accenture processes personal data for purposes including:

* Managing contractual/employment relationships
* Recruitment and talent management
* Facilitating secure, effective communication (with/without AI-based assistants)
* Operating/managing business services and operations for clients
* Legal compliance and obligations
* Monitoring use of systems to prevent fraud and reputational loss
* Social listening (market sentiment from public platforms)
* Research/analytics, including cybersecurity monitoring
* Website and network security/functionality
* Data analytics and profiling (including marketing analytics)
* Marketing products/services (unless objected to)
* Organizing events, webinars, workshops, multimedia content

**Legal bases:** Contract performance, legitimate interest (business needs, security, communication), legal obligations, and (where needed) explicit consent.

## **5. Data Sharing & International Transfers**

* Data may be shared with third parties, such as service providers (e.g., billing, payment, customer service), professional advisors, affiliates, government authorities, or clients (in connection with client-facing services).
* Transfers can include intra-group sharing (e.g., between global branches) and may cross borders—EEA to non-EEA with protection via adequacy findings, standard contractual clauses, or Binding Corporate Rules (BCRs).
* In corporate transactions (e.g., mergers, asset sales, IPO, bankruptcy), personal data may be part of transferred assets.

**Sensitive Data:** Collected only with consent or where required by law; handled with additional protections.

## **6. Data Security**

* Accenture holds ISO27001 certification, reflecting rigorous security standards.
* Security measures include strict protocols, regular third-party penetration testing, and a Client Data Protection (CDP) program.
* Security protocols cover all data, tailored by the risk category and processing type.

## **7. Data Retention**

Accenture keeps personal data only as long as necessary for the reasons it was collected, subject to:

* The lifespan of the relationship or user account
* Legal and contractual obligations
* Specific records and retention policies/procedures

## **8. Your Data Rights**

As an individual, you have the following rights (with exceptions and subject to local law):

* **Access:** Know if Accenture processes your data and obtain a copy.
* **Rectification:** Correct inaccuracies or add omissions.
* **Objection:** Ask Accenture to stop processing your data.
* **Erasure:** Have your personal data deleted when no longer needed.
* **Restriction:** Limit Accenture's use to specific purposes (e.g., with your consent).
* **Portability:** Receive your data in a common electronic format or ask for its transfer to another controller.
* **Withdraw Consent:** At any time (if data is processed on the basis of consent).

To exercise these rights, contact Accenture’s Data Privacy Officer or use designated forms/links for applicants and alumni.

## **9. Use of Personal Data on Websites & Digital Platforms**

* Data is collected directly (forms, registrations, comments) and indirectly (cookies, analytics).
* Website usage statistics include pages viewed, downloads, traffic, device info, geolocation, and system administration.
* External links/programs on Accenture sites may set different privacy standards—users should check applicable third-party privacy notices.

## **10. Cookies, Tracking Technologies, and Analytics**

* Accenture websites use cookies, web beacons, and analytics to optimize content, tailor user experience, and support marketing/content delivery.
* Users can manage cookie preferences through the site’s cookie manager.
* Cookies used may be essential, analytics-based, or marketing-focused.

## **11. Visiting Accenture Offices**

* Visitor data, including CCTV footage, may be processed for security and health/safety compliance.
* On-site visitors are given further notices about CCTV and data usage as required by law and location.

## **12. Marketing & CRM Databases**

* Accenture maintains marketing and CRM databases for business relationship management, tailored communications, and marketing analytics.
* Data may include contact details, professional info, and publicly available content (e.g., on social media).
* Recipients can manage marketing communication preferences with an opt-out mechanism at any time.

## **13. AI in Communications**

* AI tools may support Accenture’s email, chat, meetings, and collaborative platforms (e.g., drafting suggestions, real-time summaries, translations).
* Audio/video recordings and transcriptions use AI, but are only saved/processed with consent.
* Data subjects are informed if communicating with automated/AI systems.
* Personal data is not used to train, develop, or enhance AI systems unless specifically notified and anonymized.

## **14. Other Uses: Content Production/Media**

* For media production (TV/film/events), Accenture may process images, footage, health/disability data (where relevant), and participant details.
* Notices and opt-out mechanisms are made available at filming locations and to contributors.

## **15. Questions & Contact**

* Data privacy questions, right requests, or complaints should be directed to Accenture’s Data Privacy Officer (contact details in the policy).
* Individuals may also contact relevant data protection authorities or seek judicial remedy if rights are believed to have been violated.

## **Conclusion**

Accenture’s privacy policy reflects a commitment to lawful, transparent, and ethical handling of personal data—worldwide. By combining rigorous security measures, respect for individual rights, and tailored global compliance, Accenture ensures clients, partners, prospects, and employees can trust in the responsible stewardship of their information at every step.

1. <https://www.accenture.com/in-en/support/privacy-policy>