HCLTech | Supercharging Progress™

Privacy and Data Protection Whitepaper

Contents

Message from our Chief Privacy Officer 3

The Dynamic Privacy Regulatory Landscape 5

The Data Privacy Law of India – the Digital Personal Data Protection Act 5

The Regulatory Landscape – Europe, Middle East & Africa 7

The Regulatory Landscape –America & Latin Americas 10

Key Principles 12

Data Protection Officer (DPO) 13

Privacy embedded throughout the Business 15

Privacy Incident and Personal data breach management program 16

Technology 17

Training and awareness 18

Monitoring Regulatory Developments 18

Message from our Chief Privacy Officer

We have entered an exciting, dynamic chapter of data privacy. To address the ever-shifting state of affairs, the Global Privacy Office (GPO) at HCLTech is fully dedicated to ensuring that we have a robust data privacy program in place that meets current best practices set by the General Data Protection Regulation (GDPR) and other privacy laws across the globe. It is with great optimism that we enter into this new privacy landscape as a partner to our clients, with a shared goal of ensuring that our processes and policies protect the personal data we are entrusted to process both by our clients and our employees. As the Chief Privacy Officer of a cutting-edge, solution-driven, global technology enterprise, the team and I are committed to ensuring that privacy remains a top priority for our organization, and the business has the support to tackle the complexities of privacy in the new decade, today.

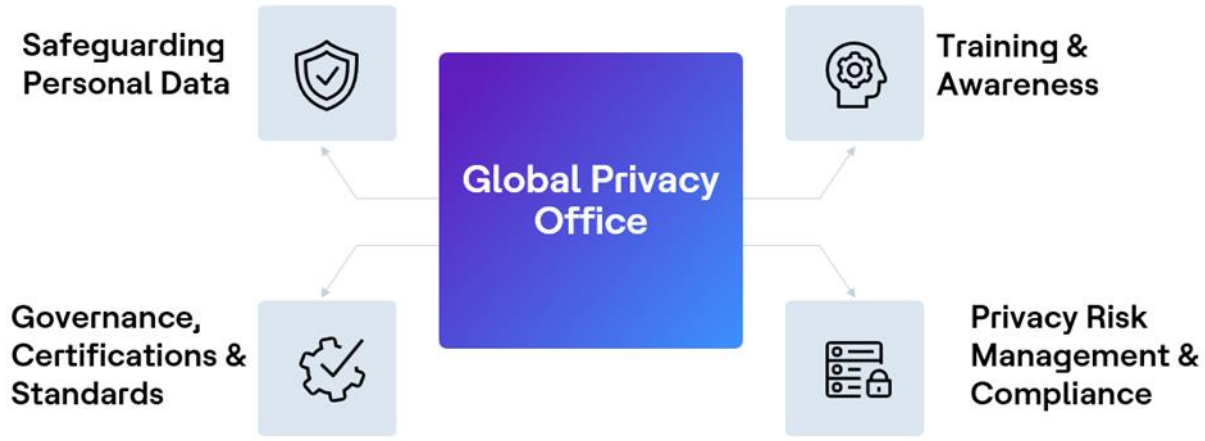
HCL's Global Privacy program – At a glance

The Global Privacy Office (GPO) is a function within the Risk & Compliance (R&C) group and is dedicated to proactively managing and implementing appropriate and effective measures to facilitate compliance with global privacy regulations and industry standards. The GPO support our client delivery teams, to ensure that they are operating within the limits of internally established privacy frameworks and contractual controls while processing personal data on behalf of our customers.

Responsibility for privacy compliance sits across all areas of the business. Every employee has a role to play with supporting data protection. The GPO works with multiple areas of the business to ensure that privacy principles are embedded in all personal data processing activities and the GPO ultimately ensures that everyone in the organization is aware of their obligations.

Continuous, cross-functional collaboration is critical to the success of our program. Our internal functional partnerships include but are not limited to, vendor risk support from our Vendor Risk Management team, contractual support from our Contract Risk Team who support who oversee our privacy contractual obligations, Information Security team for internal security controls and collaborative work with corporate/client compliance teams to identify privacy ambassadors and implement privacy risk assessments

What we do?



The Dynamic Privacy Regulatory Landscape

The Asia-Pacific region is witnessing major advancements in data privacy laws, with nations such as India, China, Indonesia, Sri Lanka, and Vietnam enacting comprehensive regulations to match global standards.
India took a major step forward by enacting its first all-encompassing data protection law, the Digital Personal Data Protection Act, 2023 (DPDP Act) on August 11, 2023. This legislation underscores the crucial role of safeguarding privacy rights and ensuring robust protection of personal data in the country.
The DPDP Act serves as an essential component alongside the Digital India Act and the Indian Telecommunication Act, addressing the governance of personal data in India. Together, these legislative measures signify a major advancement towards enhancing data protection in India's rapidly evolving digital landscape.

Like privacy and data protection laws, Artificial intelligence (AI) technology regulation in the Asia-Pacific region is also evolving swiftly, with majority of the jurisdictions having some form of AI guidelines or rules. Some countries are adopting specific laws for AI, while others rely on nonbinding principles and standards. Despite varying approaches, common policy themes include responsible use, data security, and end-user protection.

Protecting personal data and respecting privacy rights should be foundational for any global organization. This enhances value for customers and data subjects. Organizations must implement privacy by design and cultivate a culture of privacy awareness to maintain a comprehensive and adaptable global privacy program that meets evolving regulations.

The Data Privacy Law of India – the Digital Personal Data Protection Act

India enacted its new data protection law—the Digital Personal Data Protection Act, (DPDP Act) on August 11, 2023. Once in effect, the DPDP Act will replace the relevant provisions of the Information Technology Act, 2000, Information Technology (Amendment) Act, 2008, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The fundamental objective of the DPDP Act is to enhance accountability and responsibility for organizations operating in India, such as internet firms, mobile applications, and businesses dealing with the collection, storage, and processing of citizens' data. By emphasizing the Right to Privacy this legislation mandates that these entities operate transparently and are held accountable for their handling of personal data, thereby safeguarding the privacy and data protection rights of Indian citizens.

How the DPDP Act impacts businesses

The DPDP Act is the first comprehensive personal data protection law of India. It aims to align the country with the global data privacy standards and being a horizontal law, it applies to businesses across all sectors. The DPDP Act aims to regulate digital personal data and outline the duties of both the data fiduciary (organization processing the personal data) and the data principal (the individual whose data is processed). It aims to protect data principals' rights while offering organizations a robust framework for digital innovation and growth.

The DPDP Act also covers digital personal data processing outside India. It pertains to organizations providing goods or services to people in India or profiling Indian citizens, thus strengthening data protection both domestically and internationally for Indian citizens' data. Transfer of personal data outside India is restricted under the DPDP Act, thus businesses must ensure cross-border data transfers involving Indian personal data comply with the obligations set out by this legislation as well as with the specific mandates from applicable sectoral laws in India.

Like other privacy laws, the India's data protection law, outlines significant penalties for non-compliance, which can be substantial. Organizations need to be diligent in following the mandates set out by the regulations to steer clear of these penalties, as they can affect both their financial health and reputation. The DPDP Act aligns closely with international data protection standards such as the GDPR. This alignment can make compliance easier for organizations that are already following comparable regulations in different regions, contributing to a more cohesive data protection strategy.

While the DPDP Act presents challenges in terms of compliance and operational adjustments, it also offers opportunities for businesses to enhance their data protection practices and build customer trust.

How HCLTech demonstrates compliance with the DPDP Act

At HCLTech, we are well equipped to handle the evolving privacy and regulatory landscape globally, acting as both data controller and processor. Our comprehensive privacy and data protection program is based on GDPR and tailored to meet global laws like India's DPDP Act.

Our privacy program is supported by a customized, organization-wide data protection framework that aligns with business operations, data sensitivity, and applicable regulatory requirements. Robust privacy and data governance policies at HCLTech ensures data is managed responsibly and lawfully. Risk management practices on the other hand identifies and mitigates potential privacy risks through regular assessments.

HCLTech ensures efficient handling of security and privacy events through a comprehensive incident management program, minimizing client and employee

disruption. We ensure third-party vendors relied upon by us consistently comply with the applicable privacy laws through due diligence, contract clauses, and regular assessments. Furthermore, a layered defense strategy and minimum baseline controls reinforce privacy measures across all business activities at HCLTech.

An external global Data Protection Officer and regular audits by independent internal audit team and third parties enhance accountability and compliance with privacy laws, while comprehensive training program and a network of privacy champions reinforce best practices in our business operations. A user-friendly Data Subject Rights Portal empowers individuals to exercise their rights.

Alongside these measures, the Global Privacy Office at HCLTech is actively working with business units to highlight their responsibilities under the DPDP Act and to identify areas for improvement.

The Regulatory Landscape – Europe, Middle East & Africa

EU Artificial Intelligence (AI) Act

The Artificial Intelligence (AI) Act represents a significant advancement in the worldwide AI legislation, embodying the EU's aim to spearhead a thorough legislative framework that fosters the utilization of AI systems. The EU AI Act was approved at the end of May 2024 and came into effect on August 1st of the same year. Companies and other groups across industries need to make sure they maintain an up-to-date inventory of all the AI systems (regardless of whether they are developed inside the EU or outside) they are creating or implementing. The AI Act creates a tiered framework for compliance with distinct standards for each of the three risk categories (Prohibited systems, High-risk AI systems, Minimal-risk AI systems). To ascertain each AI system's risk category and the associated duties, an inventory and assessment of the systems are required. The key timelines for compliance with the provisions of the AI Act will be as follows:

- On 1st of August 2024 AI Act entered into force.
- Six months later after entry into force (2 February 2025) AI Act prohibitions will come into effect.
- Twelve months later after entry into force (2 August 2025), Requirements for GPAI (General Purpose AI) models will come into effect. However, GPAI models that were already on the market before this date will have an additional 24 months to comply.
- Twenty-four months later after entry into force (2 August 2026), Requirements for high-risk AI systems will come into effect.
- Thirty-six months later after entry into force (2 August 2027), GPAI models that were already on the market before obligations began will now have to comply.

Penalties for Non – Compliance:

There are three levels of noncompliance, each with significant financial penalties. Depending on the level of violation, the Act applies the following penalties:

- Breach of AI Act prohibitions - Fines up to €35 million or 7% of total worldwide annual turnover, whichever is higher.
- Noncompliance with the obligations set out for providers of high-risk AI systems or GPAI models - Fines up to €15 million or 3% of total worldwide annual turnover, whichever is higher.
- Supply of incorrect or misleading information to the notified bodies - Fines up to €7.5 million or 1% of total worldwide annual turnover, whichever is higher.

Analysing, predicting, and impacting human behaviour can be achieved by using various types of personal data and its processing results into valuable commodities. Automated decision-making is made possible by AI, even in areas where complex choices are necessary, using multiple factors and non-predefined criteria. However, the decisions made by algorithms can also be incorrect or biased, reflecting existing human biases and creating new ones and may lead to social implications.

The GDPR contains several provisions that pertain to AI, and certain ones are being indeed challenged by the new methods of handling personal data made possible by AI. The information made available to data subjects should enable them to understand the purpose of each AI-based processing and its limits, even without going into unnecessary technical details.

Similarities with the GDPR:

- Risk Assessments & Cybersecurity: The cybersecurity requirement of the AI Act pertains to the entire AI system rather than its individual internal components. To ensure adherence, it is essential to carry out a risk assessment that identifies the potential risks and implements required mitigation measures.
- Accountability: The AI Act brings in the idea of 'provider accountability', which holds the individuals or organization responsible for the actions of AI system they develop, deploy or operate.
- Market Principle: The AI Act's extraterritorial effect implies that organizations outside the EU may also be subject to its regulations

AI may involve the processing of personal data. The personal data of individuals can be used to help train machine learning systems, specifically in the development of their algorithm models. The use of such models can be extended in analyzing personal data in order to draw conclusions about specific individuals.

Differences from the GDPR:

- Technical and Product focused: The AI Act is a legislative measure for product safety that is designed to safeguard the safety and fundamental rights of individuals and businesses within the EU.
- Different National Authorities: In order to oversee the application and enforcement of AI Act, every EU member state must designate or create a minimum of one market surveillance authority and one notifying authority.

Consent or Pay Model

On 17 April 2024, the European Data Protection Board (EDPB), adopted its opinion on "Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms". This opinion was anticipated and welcomed by the data protection community in the EU since Facebook (currently Meta) has adapted such model as a solution to the Irish DPC's invalidation of legitimate interest and reliance on contract as available legal basis for targeted advertising.

Facebook, left with a Consent as the only possible solution, implemented it in a form of a

> The EDPB emphasizes the necessity of an alternative solution that would allow users to avoid consenting to personal data processing for behavioural advertising

visitor's choice to either agree to the data collection which would be used for targeted advertising, in exchange with the free access to the website's services or pay a fee to continue using the services provided by the website without having their personal data collected.

In its opinion, the EDPB stated that in most cases, "consent or pay" models will not be able to comply with the requirements for valid consent under the GDPR. The significance of having a balance of power between the service provider and its users is highlighted by both EDPB and UK ICO. They both noted that consent is unlikely to be given freely when there is a noticeable imbalance of power. Platforms using "consent or pay" must guarantee that individuals freely provide consent for their personal data to be processed for personalized advertising, with full awareness of the implications, and that they can withdraw consent without facing any negative consequences.

Israel's Privacy Law

On 8 August 2024, the Israeli Parliament (Knesset) passed into law the Amendment 13 the Privacy Protection Bill. The amendment includes data that would be considered as 'specially sensitive information' and as well as updates and clarifies all the essential definitions in the PPL.

> The updated Protection of Privacy Law (PPL) fortifies the defence against the increasing number of cyber threats, increases the protection of the Israeli public's fundamental right to privacy, and creates new and sophisticated arrangements and enforcement tools to meet the demands of the digital age.

The following are the notable amendments to PPL among others:

- It is included that the PPA has the authority to impose financial penalties for substantial violations of information security laws and regulations.
- The amendment establishes the requirement to appoint a privacy protection officer in public bodies and organizations whose primary function involves the processing of sensitive personal data to a significant extent, and organizations whose operations involve the systematic monitoring or tracking of individuals.
- The amendment includes to designate an internal privacy inspector for all the security agencies. The internal inspector will oversee the security body's processes and privacy protection policy, conduct privacy awareness training and report to the PPA's head
- The amendment contains a separate chapter on crimes pertaining to databases, which includes, among other things, processing data without authorization from the database owner and purposefully deceiving and individual while requesting personal data.

As part of the amendment, the obligation that applies to entities in the private sector to register the databases under their management will almost completely be eliminated, with the exception of databases managed by those engaged in information trading (in relation to public bodies, the obligation will remain in place).

The Regulatory Landscape –America & Latin Americas

United States

There is no one comprehensive data protection legislation in the United States. There are sectoral federal laws and state privacy laws. The Federal Trade Commission (FTC) is the primary regulator at the federal level. The federal sector-specific laws focus on

particular type of personal data or industry sector. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the processing and security of sensitive patient health information, the Gramm Leach Bliley Act (GLBA) regulates protection of personal information in financial industry, and the Children's Online Privacy Protection Act (COPPA) regulates the online privacy of children under the age of 13. Accordingly, the sectoral agencies are the key privacy regulators for these laws.

The United States continues to be very active in adopting comprehensive privacy laws and around 13 have been passed. California has adopted the most stringent privacy legislation, the California Consumer Privacy Act (CCPA). The CCPA, as amended by the California Privacy Rights Act (CPRA) in 2020, unlike the other state laws, applies to personal information even in the employment and business to business context, and includes a right of private action. The states also do have data breach notification laws that require breach reporting to a state agency or Attorney General under certain conditions.

Canada

In **Canada**, the bill C-27 (the Digital Charter Implementation Act) has been in discussion to reform the federal private-sector privacy law (PIPEDA) and introduce a new legislation to regulate the design, development, and use of artificial intelligence (AI) systems, .The province of Quebec has already adopted Law 25 with majority of the provisions entering into effect in 2023.

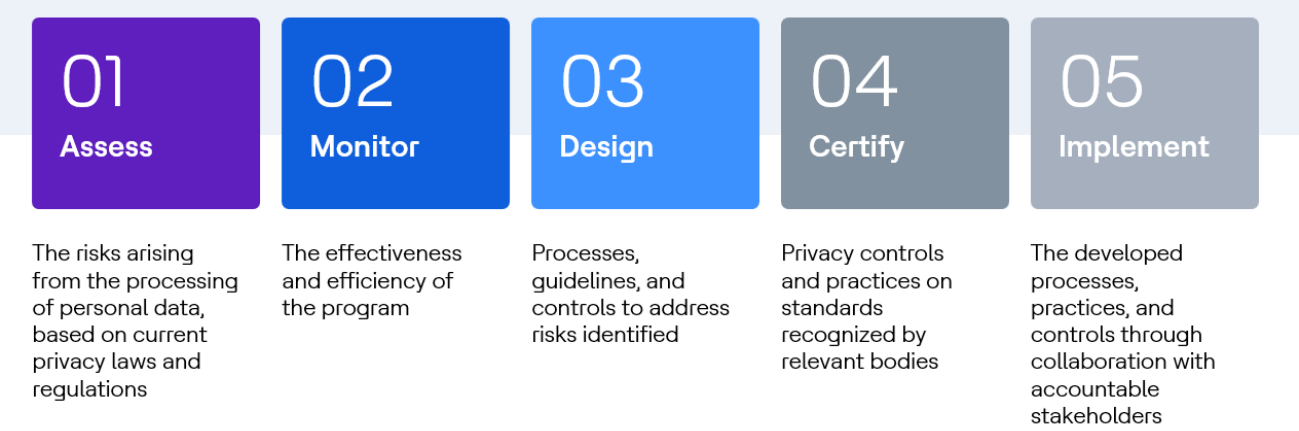
Latin America

Brazil's privacy legislation (LGPD), which became effective in 2020, bears substantial similarity to GDPR in a number of areas, including penalties for non-compliance, as well as data subject rights, and the need for privacy risk assessments. **Argentina's** privacy legislation which, became effective in 2000, prohibits the cross-border transfer of personal data from Argentina to other countries if these countries do not provide an adequate level of protection, , similar to GDPR. The Argentinian Data Protection Authority (AAIP) adopted standard contractual clauses for data transfers on October 18, 2023. In **Mexico**, the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) became effective in 2010. The LFPDPPP establish the principles and minimum standards for processing personal data and form the bases of the regulatory framework for the protection of personal data in Mexico's private sector.

Key Principles of the Global Privacy Program

HCLTech has an enterprise-wide Privacy & Data Protection Framework which consists of well-defined policies, procedures, guidance, and tools. The program covers but is not limited to: personal data inventory, policies on personal data handling, risk assessment tools, training, education and awareness, legal and program requirement gathering, data subject rights management, handling of data breach incidents, establishment of

reporting mechanisms, ongoing assessments and review of program controls. The implementation of this framework is divided into a five-phase strategy:



This approach ensures that privacy program remains agile and adapts to new international regulatory challenges and developments quickly and efficiently, as well as evolving customer expectations. This dynamic, modular, risk-based privacy framework, in conjunction with our strong cyber and information security framework, enables HCLTech to ensure compliance with applicable regulations and privacy best practices, allowing our enterprise to have a competitive advantage in the market as a business enabler.

Key Principles

Preventing Harm

HCLTech proactively identifies potential privacy risks resulting from the handling of Personal Data, as well as contractual and legal requirements, and takes remedial actions to mitigate those risks.

Management

HCLTech documents, communicates, and assigns accountability for managing its privacy framework.

Notice

HCLTech provides appropriate privacy notices explaining how it collects uses, stores, shares and disposes Personal Data.

Access and Correction

Where a legitimate request for access and/or correction of personal data is submitted by a data subject, HCLTech ensures that the request is addressed in accordance with the relevant regulatory requirement.

Use, Collection, and necessity principle

HCLTech collects and processes the data necessary to perform its contractual obligations and according to the purpose for which it was collected.

Choice and Consent
HCLTech complies with the consent and choice principle.

Monitoring and Enforcement
HCLTech monitors privacy compliance, both internally and with its vendors, and establishes processes to address inquiries, complaints, and disputes.

Quality
HCLTech ensures that the Personal Data it processes is accurate, complete, and kept up to date.

Security
HCLTech takes adequate measures to protect Personal Data from unauthorized access, data leakage, and misuse.

Cross border data transfer
HCLTech Technologies complies with applicable data transfer requirements before accessing or transferring Personal Data.

Use retention and disposal
HCLTech Technologies only uses Personal Data for the purposes identified and in accordance with any agreed privacy notices. HCLTech does not retain Personal Data longer than is necessary to fulfil the purpose for which it was collected. HCLTech disposes of Personal Data once it has served its intended purpose.

Disclosure
HCLTech Technologies discloses Personal Data to third parties only for purposes identified in its privacy notice and in a secure manner.

Data Protection Officer (DPO)

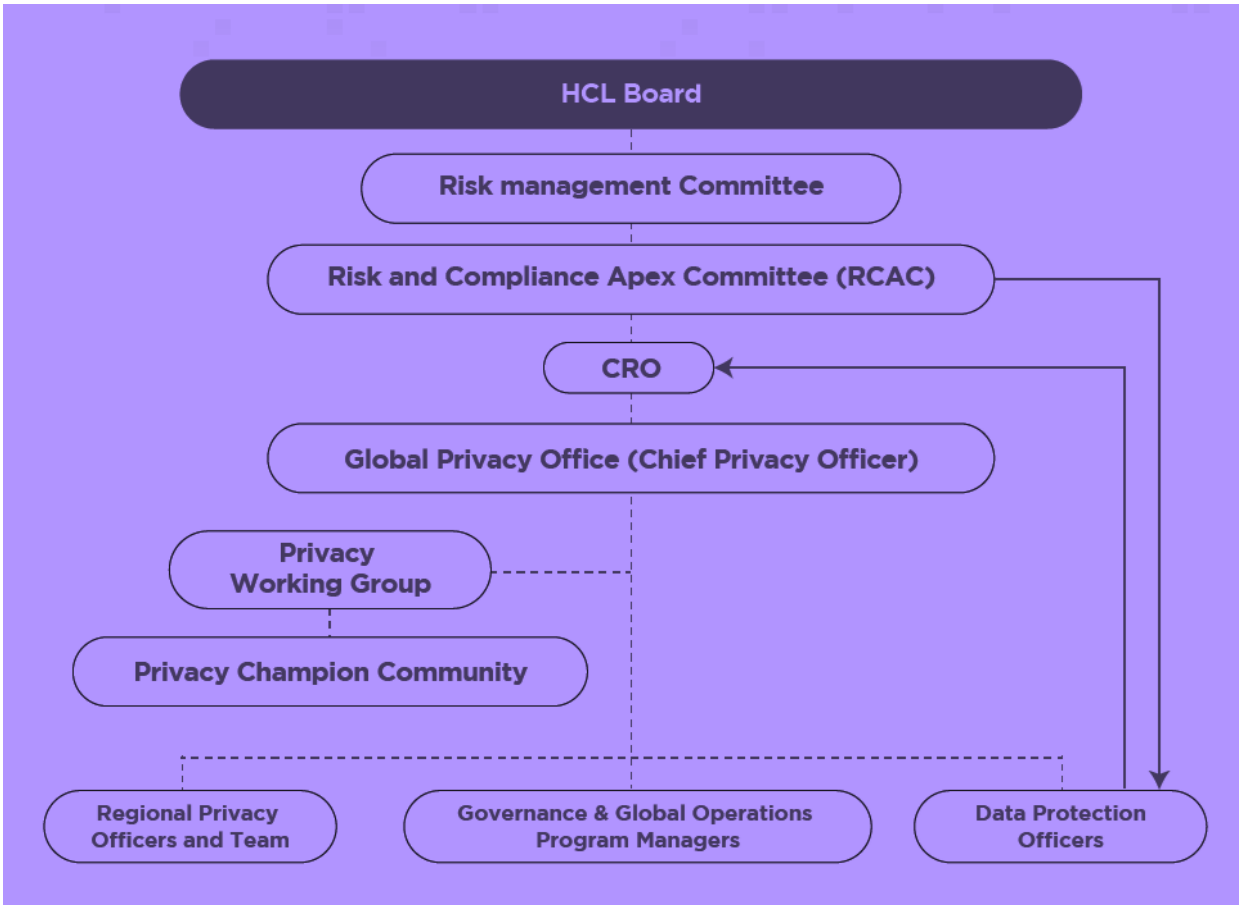
As a large, data-driven organization, HCLTech made the strategic decision to partner with Heward Mills, an external global DPO service, to act as our global DPO. This decision, among many others described in this whitepaper, demonstrates HCLTech's proactive stance on privacy and data protection. Appointing an external DPO provides assurances, accountability, and independence as is necessary for the role. It also provides HCLTech access to a wealth of resources and expertise from HewardMills' global team of professionals.

Dyann Heward Mills
HCL's Global Data Protection Officer

Heward Mills primary responsibility as DPO is to ensure that HCL processes personal data in compliance with applicable data protection laws. In pursuit of this goal, the HewardMills team has found HCL to be an active and engaged partner committed to strengthening its corporate governance, privacy operations, policies and procedures, and training. HCL's investment of time and resources into this important work ensures that it will continue to be a leader in global privacy and data protection.

Governance Structure

HCLTech demonstrates its commitment to the authority and independence of its privacy compliance oversight efforts. To facilitate the effectiveness of those efforts, it has a robust governance structure in place with clearly defined roles and responsibilities for the members of its Global Privacy Office and the wider HCLTech enterprise.



Policy Review and Approvals

The Global Privacy Office owns HCLTech's privacy policies and procedures and is responsible for updating and maintaining these policies. Any significant modifications to the privacy policies are reviewed by our Chief Privacy Officer and subsequently approved by HCLTech's Chief Risk Officer. The updated policies and related documents are then uploaded to HCLTech's Policies Hub and other appropriate platforms.

Privacy embedded throughout the Business

Privacy by Design (PBD)

Privacy by Design (PbD) is a key element of the new privacy laws across the globe. At HCLTech, privacy is not an after-thought and **privacy requirements are embedded in the early stages of a project and throughout its lifecycle**, so that the critical controls and elements of the program are in place from the outset. HCLTech has formalized the PbD framework by developing a methodology to guide the organization through the implementation process, covering HCLTech's in-house applications where we act as a data controller.

Contracting

Our privacy program is initiated as soon as a new engagement is envisaged; **we support the business and legal teams in identifying privacy risks, advise the business on best course of action and propose suitable controls to mitigate those risks**. We ensure that a data processing agreement is signed when personal data is expected to be processed by HCLTech. A data transfer impact assessment is conducted prior to any cross border data transfer in order to determine the legality and risks arising out of the proposed data transfer and, where necessary, adequate data transfer agreements are executed e.g., standard contractual clauses or IDTAs

Privacy Risk Assessments

All our service offerings, including our corporate processes, client delivery engagements, products and platforms are assessed for privacy risks using our Privacy Risk Assessment (PRA) methodology.

PRAs are conducted on all personal data processing activities and are governed by industry leading methodology and standards. The methodology provides qualitative as well quantitative insights into the privacy aspects of the data processing activities, painting a comprehensive picture of the overall risk proposition for each data processing operation.

PRAs are performed at the inception of a process – a new engagement, a new corporate process or initiative, to ensure compliance with privacy protocols from the start. **PRAs are also repeated for existing processes** at predefined intervals to ensure that privacy protocols are complied with as data processing changes to meet evolving business requirements and challenges.

Privacy Incident and Personal data breach management program

HCLTech has a long-standing commitment to privacy and information security. The mission and goal of HCLTech's Global Privacy Office is to support HCLTech's responsible use of personal data and manage global privacy risks while ensuring that HCLTech employees' and HCLTech's customers' trust is upheld. At HCLTech, the program is specifically designed to protect, monitor, and resolve threats to HCLTech and its client's data from the risks of operational disruption and unauthorized or accidental access, modification, destruction, and/or disclosure. A cornerstone of the program is centered on fostering and raising awareness on privacy and security practices along with establishing integration points with business process operations to protect all data within the purview of HCLTech.

Given the risks associated with such threats, it is HCLTech's priority to detect, respond, and recover as efficiently and effectively as possible from a potential and/or actual privacy incident. Privacy incidents at HCLTech are managed in a top-down approach, under HCLTech's overall Information Security Incident Management Program.

HCLTech's privacy incident response process is designed so that:
All employees are periodically trained and assessed on how to prevent personal data incidents from occurring, including taking steps to reduce or eliminate the unauthorized access, use, distribution, and storage of personal data.

Additionally, a specialized branch of HCLTech's Information Security team – the Cyber Security Incident Response team (CSIRT) – lends a great deal of sophistication to the management of privacy incidents, focusing on cyber-analytics and forensic investigations of our organizational network. Through our internal escalation process and our network of skilled security professionals, HCLTech is well-prepared to mitigate the impacts of a potential personal data breach and proactively meet the challenges of unforeseeable threats.

Technology

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust (OT) the industry leading platform to operationalize privacy, security, and data governance is the platform of choice for HCLTech. OneTrust has regulatory intelligence baked into its assessment templates which HCLTech has customized for our privacy program. We utilize the automated assessment module to conduct privacy risk assessments at scale and create a data map of the personal data we process across the organization. Additionally, HCLTech leverages OT data subject rights' module, Benchmarking & Maturity Assessment and Data Guidance as our regulatory research engine.

Training and awareness

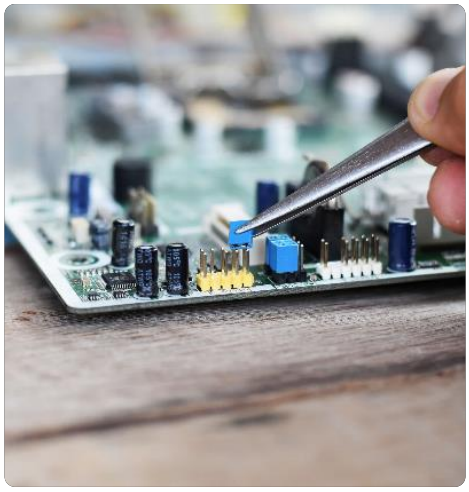
The Global Privacy Office prides itself on pursing ways to enhance knowledge and awareness of data protection throughout the organization. Employees and third-party resources are required to undergo a mandatory enterprise-wide privacy training, which addresses key privacy concepts, principles, laws, best practices, and contractual obligations. In addition, HCLTech has partnered with OneTrust to offer role-based, tailored, privacy training programs providing specific guidance to employees within their respective functions. We work closely with external training providers to customize and update our trainings as and when there are any new regulatory developments. Training compliance status is also tracked, monitored and reported to executive leadership.

Privacy Awareness is a key component of our program. We take every opportunity to engage our global workforce by implementing year-around awareness campaigns including corporate-communications, global circulation of newsletters, leveraging social media channels with data privacy content, live-events, virtual & in-person activities.

In continuation of fostering a privacy mindset and engraining privacy culture throughout the organization, the Global Privacy Office has created an expansive network of Privacy Champions that provide departmental privacy support. This community encompasses professionals who help embed and reinforce privacy knowledge and best practices. Furthermore, our partnership with the International Association of Privacy Professionals has allowed us to train our privacy champions through a live, intensive CIPP/E program for over 400 participants.

Monitoring Regulatory Developments

Part of being a cutting-edge IT services company means knowing how to evolve with the regulatory landscape. HCLTech has designed its Privacy Program considering global privacy regulations that govern the collection, use and handling of personal information and derived privacy principles from the GDPR. and Generally Accepted Privacy Principles. The Global Privacy Office at HCLTech continuously monitors changes in the regulatory framework by performing periodic regulatory updates review, risk assessments, issuing advisory and implementing control.



Key Differentiators

Trust is increasingly becoming a parameter of success and establishing a comprehensive privacy program is paramount for any organization. HCLTech's global privacy program is designed, implemented and maintained by well-resourced, subject matter experts from around the globe. Our distinguished team of diverse, privacy professionals are globally dispersed with access to key business stakeholders within their respective regions, bringing a broader, more holistic perspective and a variety of privacy compliance solutions to the table. Our world-wide exposure has allowed us to efficiently and effectively operationalize and sustain our long-term goals as a privacy program.

The HCLTech Global Privacy Office has also leveraged various platforms, technologies and forums including the International Association of Privacy Professionals (IAPP), OneTrust, Data Guidance, Lexology, Data Security Council of India (DSCI) and outside counsel to name a few. These third-party relationships have truly streamlined and uplifted our program through automation, advancement, continuous support, and guidance.

Below, you will find a summary of key differentiators that drive and further elevate our program:

KEY DRIVERS	DESCRIPTION	ACCESSIBILIY	
Global Privacy office SMEs	Consists of subject matter experts that are situated globally	224,756 Employees, Clients	☑
OneTrust Program	Automation of Privacy Risk Assessments	Global Privacy Office & Privacy & Security Champion Network	☑
Data Protection Officer	Independent, Third-party, oversight and guidance (Heward-Mills Ltd)	Global Privacy Office, 224,756+ Employees, Clients	☑

Data Guidance	Privacy Research Platform	Global Privacy Office	☑
Privacy Trust Center	Client-facing Trust Center showcasing our privacy posture and program Privacy Trust Center | HCLTech	Externally-facing	☑
IAPP Membership	A global information privacy community and resource	Global Privacy Office & Privacy & Security Champion Network	☑
Mandatory Privacy training	Comprehensive privacy training program mandated annually for all HCLTech employees	224,756+ Employees	☑
Mandatory HIPAA training	Comprehensive HIPAA training program mandated annually for Life Science, Pharma & Healthcare divisions	HCLTech Life Science, Pharma, Healthcare	☑
Role-Based training	LIVE, function-specific data privacy trainings (e.g. HR, Finance, Legal, Marketing etc)	224,756+ Employees, Privacy & Security Champions	☑
Year-Long Privacy Awareness Campaign	Privacy promotional materials distributed year-round (mailers, live events, newsletters etc.)	224,756+ Employees	☑
Privacy & Security Champion Network	Community of 1000+ privacy ambassadors both on the delivery and corporate sides	Privacy & Security Champions	☑
Global Privacy Portal	A one-stop shop microsite, hosted internally with expansive resources Trust Arc TRUSTe, SOC2	224,756+ Employees	☑
Certifications	Trust Arc TRUSTe, SOC2 Type 2 (Privacy Trust Principles), ISO 27001	224,756+ Employees via public facing HCLTech websites	☑
Continuous Improvement	Routine privacy program uplift, maintenance of KPIs, leadership buy-in		☑

224k
Ideapreneurs

13.8B
Revenue

60
Countries

HCLTech | Supercharging Progress™

hcltech.com