HCLTech | Supercharging Progress™

Privacy and Data Protection Whitepaper

Table of Contents

Message from our Chief Privacy Officer

We are entering an exciting, dynamic chapter of data privacy. To address the ever-shifting state of affairs, the Global Privacy Office (GPO) at HCLTech Technologies 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.

The Dynamic Privacy Regulatory Landscape

More than 3 years have passed since the GDPR came into effect and it is fair to say that this sweeping regulation has laid the foundations of the current privacy regulatory landscape.

We have seen a tangible shift in countries rolling out new privacy laws and regulations (e.g., Brazil's LGPD and China's PIPL), which in most cases mirror the principles of the GDPR. This shift in global standards showcases the importance of valuing privacy rights and adequately protecting personal data, and it is a standard that is only going to expand across the globe. The protection of personal data and valuing the privacy rights of individuals should be seen as a baseline for any global organization, regardless of where it operates. This is a key differentiator and value add to both customers and data subjects.

The Covid-19 pandemic impacted individuals, businesses, and countries on a large scale. This unprecedented virus, caused ripple effects in industries and governments on how to tackle the threat of the virus, moving to remote working, and how to appropriately handle and share vast amounts of health-related data. The privacy programs of global organizations had to navigate varying guidance from regulators on how to process their employee health data, which made it imperative that organizations have fully resourced privacy programs with trained privacy experts. The exponential move to working from home and digitalization has also posed challenges for organizations, especially on how to adequately protect personal data.

> To alleviate this challenge for HCLTech, the Global Privacy Office was a key stakeholder in HCLTech's enterprise pandemic response initiatives and constituted a Covid Taskforce comprising of privacy experts from different GEOs to research, assess and advise the business on the evolving requirements for handling personal and sensitive personal data.

It is imperative that organizations embed privacy by design, and a culture of privacy awareness in all facets of their business so their global privacy program can be agile and better support the business with the dynamic regulatory landscape.

The Regulatory Landscape – Europe, Middle East & Africa

Standard Contractual Clauses

In June 2021, the European Commission published a modernized, GDPR aligned version of the Standard Contractual Clauses (SCCs). The SCCs are a set of data transfer agreements that are relied upon for the legitimate transfer of personal data from the EEA to countries outside of the EEA. These revised clauses brought elevated harmony between data protection and data transfer to non-EU/EEA and non-adequate countries such as United States, India, Singapore etc. The revised SCCs bring a closer alignment with the GDPR by including provisions for greater detail on security measures, rights of recourse for data subjects, and governing law. On the flip side, it did and continues to put a significant administrative and financial burden on every organization relying on SCCs, including establishing org-wide programs to revise the already executed contractual arrangements.

> In its Schrems II judgement of July 2020, the Court of Justice of the European Union (CJEU) decided that, while the most commonly used data transfer mechanism also known as EU Standard Contractual Clauses (SCCs) remain a valid option, there is also a need to assess, on a case-by-case basis, whether the personal data being transferred will be adequately protected

The free flow of personal data from the EEA to non-adequate countries continues to be a hot topic in Europe, and the landscape remains volatile as the free flow of data to the United States remains a contentious issue. Further, CJEU suggested that data transfer impact assessments should be carried out for any non-EEA data transfers. First, to assess the legal regime of the non-EU/EEA country and the ability of government bodies in that country to get access to EU personal data and second, the cooperation mechanisms under which the EU data subjects will be able to enjoy effective and enforceable rights, along with the ability to seek judicial redress. Although, assessing the equivalent safeguards of data protection in a third country is not a new concept, the

requirement of conducting such an assessment prior to data transfers has become more ubiquitous and demanding in this digitally connected world.

> Outside of Europe, The Protection of Personal Information Act (or POPI Act) is South Africa's answer and equivalent of the GDPR.

The next significant update for data privacy in the EU is likely to be EU Commissions proposal for a new EU Privacy and Electronic Communications Regulation which is currently under reviewThis regulation will provide provisions on electronic communications content, direct marketing practices (including cookie management), and metadata carried out in connection with the provision and use of electronic communications services. The management of cookies and consent for cookies remains a topical issue in Europe, so it is prudent for organizations to remain up to date with relevant case law and judgements and monitor developments closely and assess the impact for your business.
It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully collect, process, use, store or delete the personal data of natural persons.

The Regulatory Landscape –America & Latin Americas

The Federal Trade Commission (FTC), effectively the US federal privacy regulator, has announced its plan to update many of its rules and guidance. FTC rulemaking in 2022 could focus on the reviews of the rules and guidelines including the Children's Online Privacy Protection Rule, the Health Breach Notification Rule, the Identity Theft Rules, the Telemarketing Sales Rule, and the Safeguards Rule.

> In the United States, it remains the case that there is no single, comprehensive federal law regulating privacy and the collection, use, processing, disclosure, and security of personal information

Brazil's privacy legislation, which became effective in 2020, bears substantial similarity to GDPR in number of areas, including penalties for non-compliance, as well as data subject rights, and the need for privacy risk assessments. In

Canada, while updates to federal privacy legislation died in Parliament in 2021, the province of Quebec adopted Bill 64 with provisions due to enter into effect over a three-year period, starting in 2022. In particular, breach notification provisions of Bill 64 enter into effect in September 2022, along with other requirements.

The Regulatory Landscape –Asia Pacific (APAC)

Countries in this region continue to work together towards synchronization of data privacy requirements, such as with the ongoing adoption of the EU GDPR and by uplifting their data protection regimes to match the global standards.

New Zealand, Singapore, Japan, and the Philippines are in the process of amending their existing privacy legislation to strengthen obligations around individual rights, privacy awareness, transparency, breach reporting, data protection safeguards, cross-border data transfers, etc. Most APAC countries impose restrictions on cross-border transfers and only allow such transfers through limited legal mechanisms, such as adequacy decision, consent, legal requirements, contracts, or binding corporate rules. Japan, New Zealand, and South Korea have obtained an EU adequacy decision. HCLTech operates from many APAC countries and therefore it is imperative for HCLTech to navigate a diverse set of privacy and data protection regulatory requirements in this region and identify appropriate privacy obligations and ensure its data processing activities are in compliance with applicable legislation.

Privacy laws in the Asia Pacific 'APAC' region differ considerably

Countries like India, China, and Indonesia are developing comprehensive data privacy laws that aim to offer an equivalent level of personal data protection as the EU GDPR

HCLTech'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.

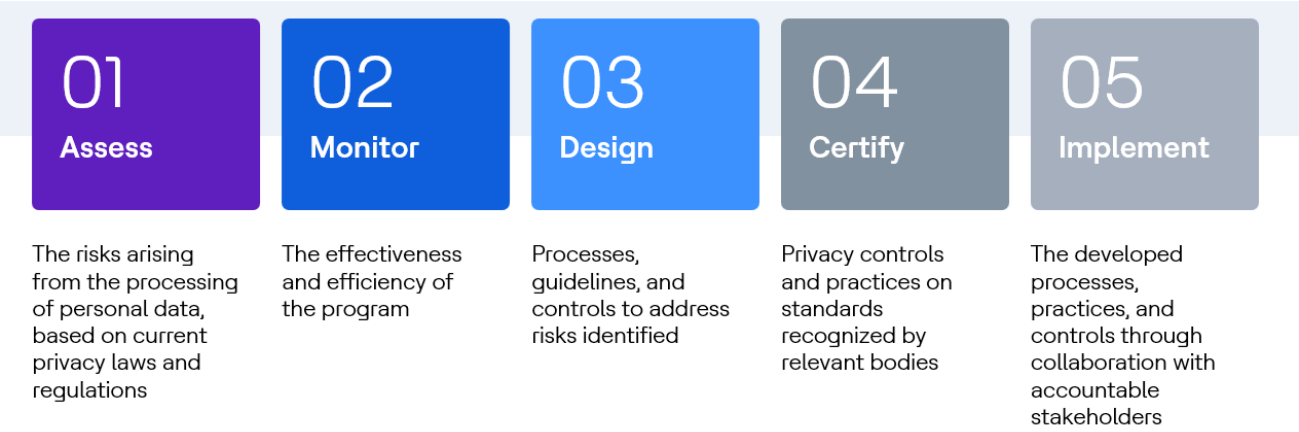
Responsibility for privacy compliance sits across all areas of the business. Every employee has a role to play with supporting data protection. The Global Privacy Office works with multiple areas of the business to ensure that privacy principles are embedded in all personal data processing activities 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, Contract risk 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?

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)

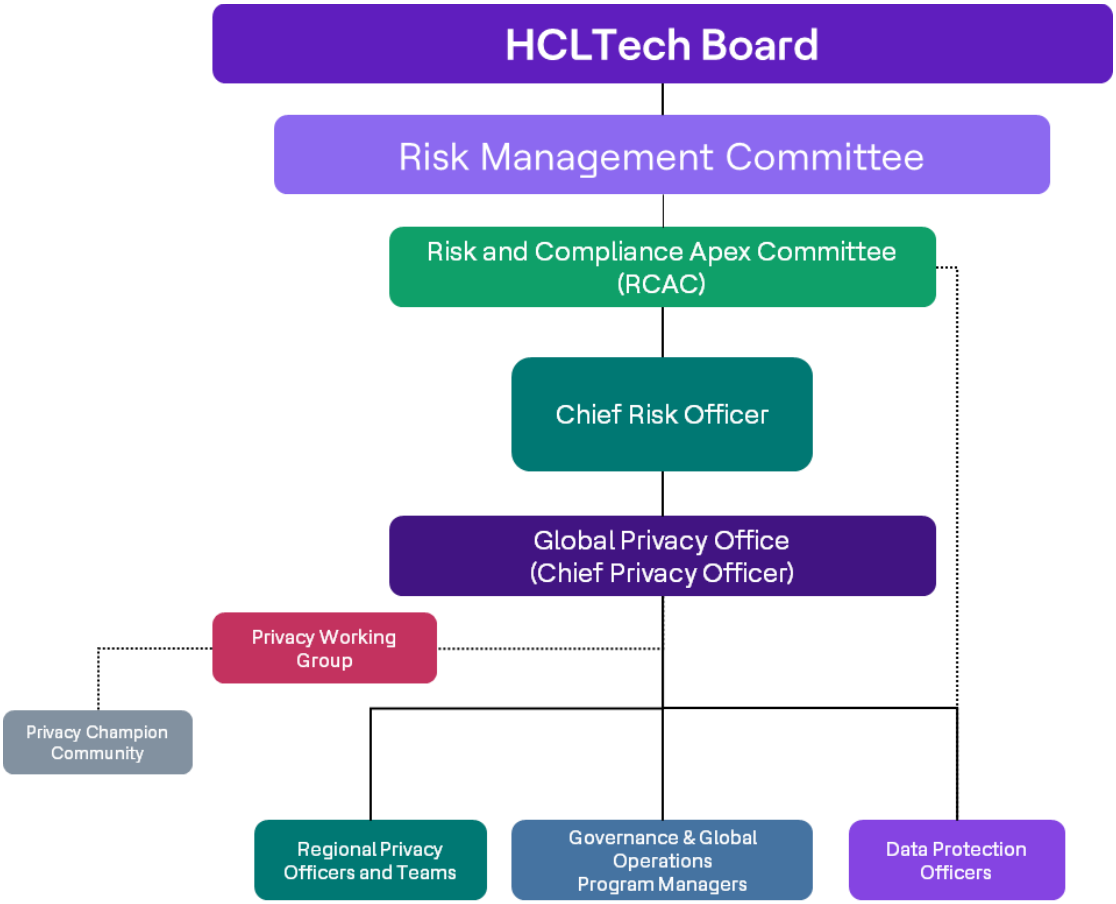
As a large, data-driven organization, HCLTech made the strategic decision to partner with Heward Mills, an external global DPO service, to act as our global DPO. This decision, among many others described in this whitepaper, demonstrates HCLTech's proactive stance on privacy and data protection. Appointing 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 Heward-Mills' global team of professionals.

Dyann Heward Mills
HCLTech's Global Data Protection Officer

"Heward-Mills primary responsibility as DPO is to ensure that HCLTech processes Personal Data in compliance with applicable data protection laws. In pursuit of this goal, the Heward-Mills team has found HCLTech to be an active and engaged partner committed to strengthening its corporate governance, privacy operations, policies and procedures, and training. HCLTech'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."

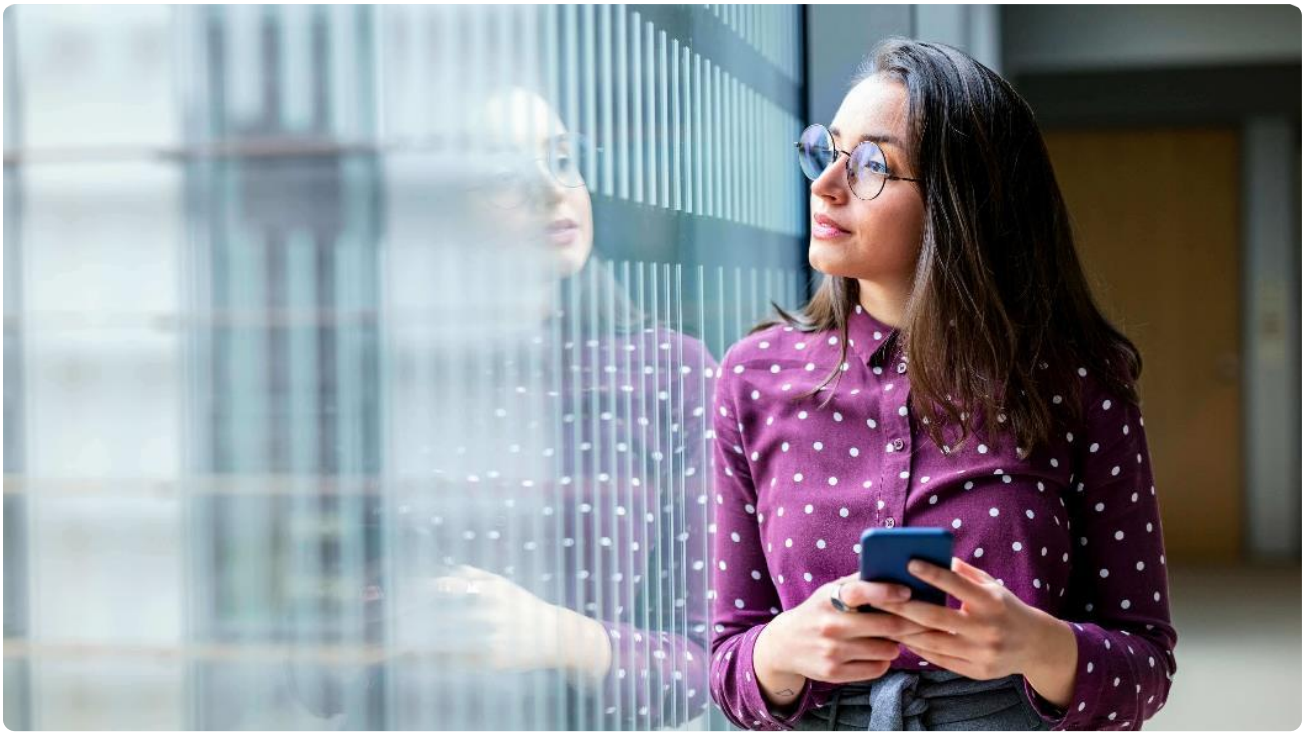
Governance Structure

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. The Privacy Working Group and the Risk & Compliance Apex Committee review privacy policies and related procedures on a periodic basis. 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, and where necessary adequate data transfer agreements are executed e.g., standard contractual clauses. In line with the updated SCCs, a data transfer impact assessments are also conducted prior to any data transfer.

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 development. training compliance status is tracked 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.

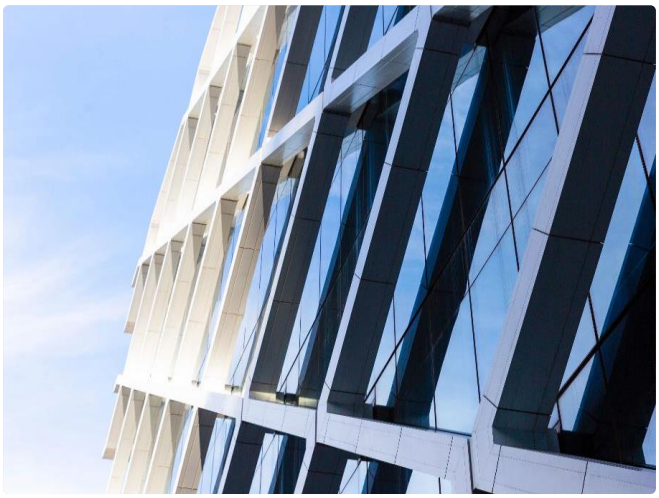
In continuation of fostering a privacy mindset and engraining privacy culture throughout the organization, the Global Privacy Office has created an expansive network of Privacy Champions that provide departmental privacy support. This community encompasses professionals who help embed and reinforce privacy 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 Centre for Information Policy Leadership (CIPL), the International Association of Privacy Professionals (IAPP), OneTrust, Data Guidance, 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	223,400+ Employees, Clients	☑
OneTrust Program	Automation of Privacy Risk Assessments	Global Privacy Office & Privacy Champion Network	☑
Data Protection Officer	Independent, Third-party, oversight and guidance (Heward-Mills Ltd)	Global Privacy Office,223,400+ Employees, Clients	☑
Data Guidance	Privacy Research Platform	Global Privacy Office	☑
CIPL Membership	Global privacy think tank made up of leaders, authorities and policy makers	Global Privacy Office	☑
IAPP Membership	A global information privacy community and resource	Global Privacy Office & Privacy Champion Network	☑
Mandatory Privacy training	Comprehensive privacy training program mandated annually for all HCLTech employees	223,400+ Employees	☑
Mandatory HIPAA training	Comprehensive HIPAA training program mandated annually for Life Science, Pharma & Healthcare divisions	HCLTech Life Science, Pharma, Healthcare	☑
Role-Based training (OneTrust)	Function-specific data privacy trainings	223,400+ Employees, Privacy Champion	☑
Year-Long Privacy Awareness Campaign	Privacy promotional materials distributed year-round (mailers, live events, newsletters etc.)	223,400+ Employees	☑
Privacy Champion Network	Community of 1000+ privacy ambassadors		☑
Global Privacy Portal	A one-stop shop microsite, hosted internally with expansive resources Trust Arc TRUSTe, SOC2	223,400+ Employees	☑
Certifications	Trust Arc TRUSTe, SOC2 Type 2(Privacy Trust Principles), ISO 27001	223,400+ Employees via public facing HCLTech websites	☑
Continuous Improvement	Routine privacy program uplift, maintenance of KPIs, leadership buy-in		☑

HCLTech | Supercharging Progress™

hcltech.com