Gap Assessment – Personal Information Protection and Electronic Documents Act (PIPEDA) & Quebec Law 25 – EXECUTIVE SUMMARY

Prepared for

(FINAL VERSION)

Prepared by Ralph T O'Brien,
Fellow IAPP, CIPP/US/E, CIPM, CIPT, CDPSE, ECPC-B DPO
Principal Consultant
Carried out Nov 2024, Report Dec 2024

Executive Summary

Tuya Smart (TUYA or “the company”) is a private sector company that focusses on a cloud platform as a service infrastructure (PaaS) and a range of both software and hardware products . TUYA collects, uses, discloses, stores and disposes of personal information as part of its ongoing business operation. TUYA operations include processing personal data within Canada including within the province of Quebec, and therefore seek assurance on the organisations management of personal data in regards to their corporate response to the relevant legislation.

Canadian private sector companies are subject to the provisions of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which is overseen by the Privacy Commissioner of Canada. PIPEDA's 10 Fair Information Principles form the "ground rules" for how companies must collect, use and disclose personal information, as well giving access, correction and redress rights to the individuals to whom that information belongs. In addition the Quebec province has passed an additional law 25 that applies to the private sector in September 2021 that modernises and introduces new requirements similar to what we have seen raised worldwide with laws such as the EU General Data Protection Regulation or GDPR.

To better understand privacy risks posed regarding TUYA’s compliance with PIPEDA, and to chart a course for mitigating or managing these risks as needed, TUYA has engaged TrustArc to undertake an assessment of its current risk profile, identify any gaps, and map a strategy for bringing the organization to its preferred privacy posture. This report and its supporting materials constitute the primary TrustArc deliverable to TUYA.

TUYA’s compliance with PIPEDA's Fair Information Principles and Quebec Law 25 were assessed in November 2024 using surveys, document review and follow-on questioning of subject matter experts. This high-level assessment is designed to identify gaps in TUYA’s privacy program and offer corresponding remedial steps to improve compliance with PIPEDA.

Canadian laws requires organizations that collect, use, disclose, retain and dispose of personal information to adopt a sound and comprehensive privacy program. This program should include points of accountability and escalation, training, and documentation to assist employees and demonstrate the importance TUYA places on the safeguarding of all personal information in its custody.

A strong privacy program features a sense of collective accountability, a "culture of privacy" across all levels of the organization supported by policies, procedures and training which leave no doubt as to the employee’s responsibilities toward the safeguarding of privacy rights.

Findings Overview

The responses from TUYA indicate an overwhelmingly compliant standpoint, with the limited respondents giving positive responses to every question, there has been activity since 2022, with documents being updated

throughout 2023. The organisation has engaged really positively and has endeavoured to produce whatever evidence of implementation and documentation has been requested.

The Consultant has tried to seek evidence that this evidence was in place effectively, but this was difficult due to the remote nature of the methodology, and a narrow view of the organisation through the single respondent assigned. With the experience gained from dealing with many large global multinational organisations over decades have never before encountered a "perfect score" due to the risk based nature of Data Protection law.

Culturally it is understandable that an organisation may wish for perfection and have a completely perfect response, but this may come at a cost of taking a more realistic view and achieving long term benefit. Whilst the desire for perfection is commendable, and the company could provide some evidence of implementation, TrustArc encouraged the Company to expose the Consultant to lower level evidence of implementation. This then identified some improvement opportunities for the organisation in terms of being assured of systematically incorporating areas of their privacy programme consistently and programmatically, such as Privacy Notices, Privacy by Design, DPIAs, International Transfer and Third Party Management. The results of these activities then require review for further product and service enhancements and ongoing compliance monitoring.

Whilst there is policies and documentation in place, there remains the question of implementation into a wider Data Protection programme. To strengthen the company's alignment with PIPEDA's Fair Information Principles and the new Quebec law, TrustArc recommends that TUYA also carry out a lower level implementation review in addition to this report to assess whether the documentation privacy program framework supplied is, in fact effectively in place for each of its products and services, as part of a co-ordinated company wide programme.

Whilst there are no new findings TrustArc would like to re-iterate the findings from the previous report for review and highlight areas of progress made. It seems that whilst compliance efforts have been reviewed and progress made, there remains some areas of improvement still to pursue . We restate these recommendations for convenience.

By taking the recommended steps to reveal and uncover elements of non-conformity and non-compliance within the organisation, TrustArc believes TUYA could better engender a culture of privacy throughout the organization, and enhance the product and service offerings to its customers.

Updated Recommendations Summary

REF	Recommendation	Timeframe
REC 1	Implement ongoing privacy governance and oversight at the executive level. ***UPDATE: Evidence provided of security compliance committee that includes data protection issues being discussed at senior level and actioned accordingly.***	CLOSED

REC 2	Revise Data Protection Policy for whole business programme	<3 months
REC 3	Further simplify and develop more user friendly outward-facing Privacy Notices	6 months
REC 4	Update and maintain the inventory of all personal information collected and used by the company	6 months
REC 5	Formalize Vendor Management data protection requirements **UPDATE: Evidence provided of Data Security Assessments and Contractual Data Processing Addendums. Whilst some Data Protection content is included, further questions could be developed and added.**	12 months
REC 6	Formalize a full DPIA process with evidence of implementation **UPDATE: Evidence provided on DPIA completion as part of development process, that results in controls being implemented to prevent harm to individuals.**	CLOSED
REC 7	Implement as part of the Data Inventory/Mapping an understanding of international transfers and appropriate transfer mechanisms. **UPDATE: Evidence provided of international transfers identified and justified.**	CLOSED
REC 8	Implement a corporate record management program that ensures the secure storage and eventual destruction of personal information collected by the company. **UPDATE: Evidence provided of retention and disposal programme**	CLOSED
REC 9	Extend a wider Privacy programme to all process (e.g., Human Resources, Sales, Customer Service, Payroll Services etc.) that collects and uses personal information. **UPDATE: Evidence provided of HR, sales, customer services data protection audit records etc.**	CLOSED
REC 10	Instigate processes to deal with deceased individuals	12 months
REC 11	Age Verification services	12 months
REC 12	Reporting on Rights Requests status as part of co-ordinated wider programme	12 months

For further information and detail on the recommendations, please see the full report page 29-32

After TUYA has reviewed this Report, we encourage questions, feedback, corrections, and supplementation prior to finalization. If TUYA chooses to implement the recommendations that we made in this Report, TrustArc would be pleased to work with the Company to review those changes and is available for additional engagements as TUYA implements the recommendations.

Appendix – About TrustArc

Founded in 1997, TrustArc has a history and depth of experience in data privacy management that is unmatched by any other company on the market. We deliver the most comprehensive suite of Data Privacy Management Services available, leveraging the power of the TrustArc Data Privacy Management Platform.

Extensive European Regulatory Experience

Since our founding in 1997 as TRUSTe, we've built strong relationships working with regulators and privacy organizations worldwide. TrustArc maintains an ongoing dialogue with regulators around the world to promote the recognition of accountable data compliance and transfer mechanisms. In the EU, TrustArc regularly participated in the Article 29 Working Party meetings that led to the development of the GDPR language, and with APEC economies on global interoperability, along with key stakeholders who have sought or are seeking approval of their BCRs, including IBM, Hewlett-Packard and Merck. In addition, TrustArc has a leading role in the Centre for Information Policy Leadership's (CIPL) working group on GDPR implementation.1 The outcomes of this work will be formally submitted to European regulators on behalf of industry in advance of the formal implementation of the GDPR.

TrustArc has also worked with CIPL members on the US-EU Privacy Bridges Project (https://privacybridges.mit.edu/). TrustArc also regularly engages with regulators in the Asia-Pacific region on cross border interoperability with European regulators through a variety of fora, including as a delegate to the biannual APEC conferences.

On the ads compliance front, we work closely with self-regulatory agencies such as the European Interactive Digital Advertising Alliance (EDAA) in the development of the EU Self-Regulatory Programme for OBA. TrustArc is on the Advisory Board of the IORMA Global Consumer Commerce Center with close links to UK Trade and Industry.

[1] https://www.huntonprivacyblog.com/files/2016/05/CIPL-GDPR-Project-Description.pdf

European Presence

TrustArc opened its first European Headquarters in London in 2012 and over the intervening years has built an extensive network of privacy technology and consulting clients, law firm partners, and continues to host and/or participate in major data protection events across Europe.

Large / Loyal Client Base & TrustArc's Consumer Brand

TrustArc clients are part of a proud and loyal network of thousands of companies worldwide that benefit by being associated with some of the most respected brands. Our clients choose to associate with the ubiquitous TRUSTe brand and Certified Privacy seal programs, recognized by consumers worldwide and displayed on millions of web pages, ads, and apps each month. TrustArc, through our TRUSTe brand, provides certified companies with access to the leading privacy assurance program as a part of demonstrating their commitment to privacy.

Robust Technology Platform

Built by veterans from leading privacy, security and ad tech companies, and used in-house to support thousands of clients, our one of a kind SaaS-based Data Privacy Management (DPM) Platform delivers innovative technology capabilities to power all phases of DPM from conducting assessments, to implementing compliance controls, to managing ongoing assurance surrounding privacy.

Deep Bench of Privacy Expertise

We are recognized data privacy experts with significant experience leading global privacy assessments for large enterprises. TrustArc has more employees holding CIPP, CIPM, and the prestigious FIP designation, than any other organization in the world. Many of our privacy professionals have law degrees, and all have experience as privacy practitioners at the highest levels in major corporations, with experience as privacy leaders and consultants to companies like IBM, Citrix, Yahoo, Merck, Intel, Intuit, Microsoft, Kellogg's, American Express, Pfizer, Kimberly-Clark, HSBC Bank, Hertz, Comcast, Adobe Systems, and government agencies.

Who We Help

TrustArc's past and present client roster includes: