How can data trust make you more competitive in the digital economy?

The imperative for Canadian companies to build a robust data trust environment

The better the question.
The better the answer.
The better the world works.

Building a better working world

Canada's data protection landscape is changing. Whether it's proposed new privacy regulations such as Bill C-11 or Bill 64, data breach fines, criteria for privacy certifications or responding to consumer expectations, the reality is that there are many reasons for organizations to seriously think about the way they collect, process and protect data. One of the main objectives of Canada's Digital Charter is to help companies be successful and competitive in the digital economy while building consumer trust.

For the next normal, people are expecting organizations to be kind and think human. Recognizing the relevance of privacy brings the individual to the centre of the conversation to create trust and generate value beyond just compliance or risk reduction. **The question should not be why, but how.**

Today's business decisions are data driven. How effective these decisions are will depend in the accuracy of the data. How human they are will depend on getting the proper consent from the individuals impacted, as well as full commitment from other stakeholders involved in properly protecting data and making decisions on their processing based on a well thought set of principles. This is data trust, the action of using data with all stakeholders in mind and based on four fundamental pillars: stewardship, ethics, protection and privacy.

By defining a proactive data trust strategy that incorporates effective privacy elements, organizations can achieve the following benefits:

- Incorporation of controls earlier in the design of processes and tools to increase effectiveness and reduce costs
- Identification of privacy value generators for key stakeholders
- Increased trust in the organization's brand by creating trust by design

How can you convert data risk into data trust?

The expected evolution of the Canadian privacy landscape creates an opportunity to transform data risk into data trust, to exchange risk reduction for value generation. Canadian organizations can start setting the ground for solid data trust by paying attention to three fundamental considerations:

1. Understand the data your organization processes

Creating data trust starts with understanding the data collected, stored and used by all the processes across your organization. This is a fundamental activity not only for data trust in general, but for privacy in particular, since it's complicated, if not impossible, to protect data you don't know you have.

2. Be kind, think human

For data trust to be generated, people need to be at the centre of the conversation, guiding how decisions are made so that all stakeholders get the benefits of corporate data processing, making privacy recognized as a human right and creating value for everyone connected to your organization.

3. Get support from enabling technology

Responding to privacy compliance obligations and transforming the associated activities into value generators and trust requires technology. You might need new and specific tools to manage privacy and data protection, but before going there you need to understand the tools your organization is using now so you can explore how they can be used to generate data trust.

1 Understand the data your organization processes

Data trust is a response to consumers' shifting mindset after the COVID-19 lockdowns. For data trust to be generated, your organization needs to build strong alliances, starting with the Privacy Officer and the Cybersecurity Officer. These executives need to work hand in hand to interact with business process owners so they can clearly identify how data flows across the organization.

Communication is one of the challenges. As we reported in the EY Global Information Security 2020 survey, the Cybersecurity Officer tends to have a relationship with IT that is characterized by high trust and consultation. But the same cannot be said when it comes to other departments like marketing, product development, finance or privacy.

In our latest research, we found the following were top privacy awareness drivers for consumers:

43%

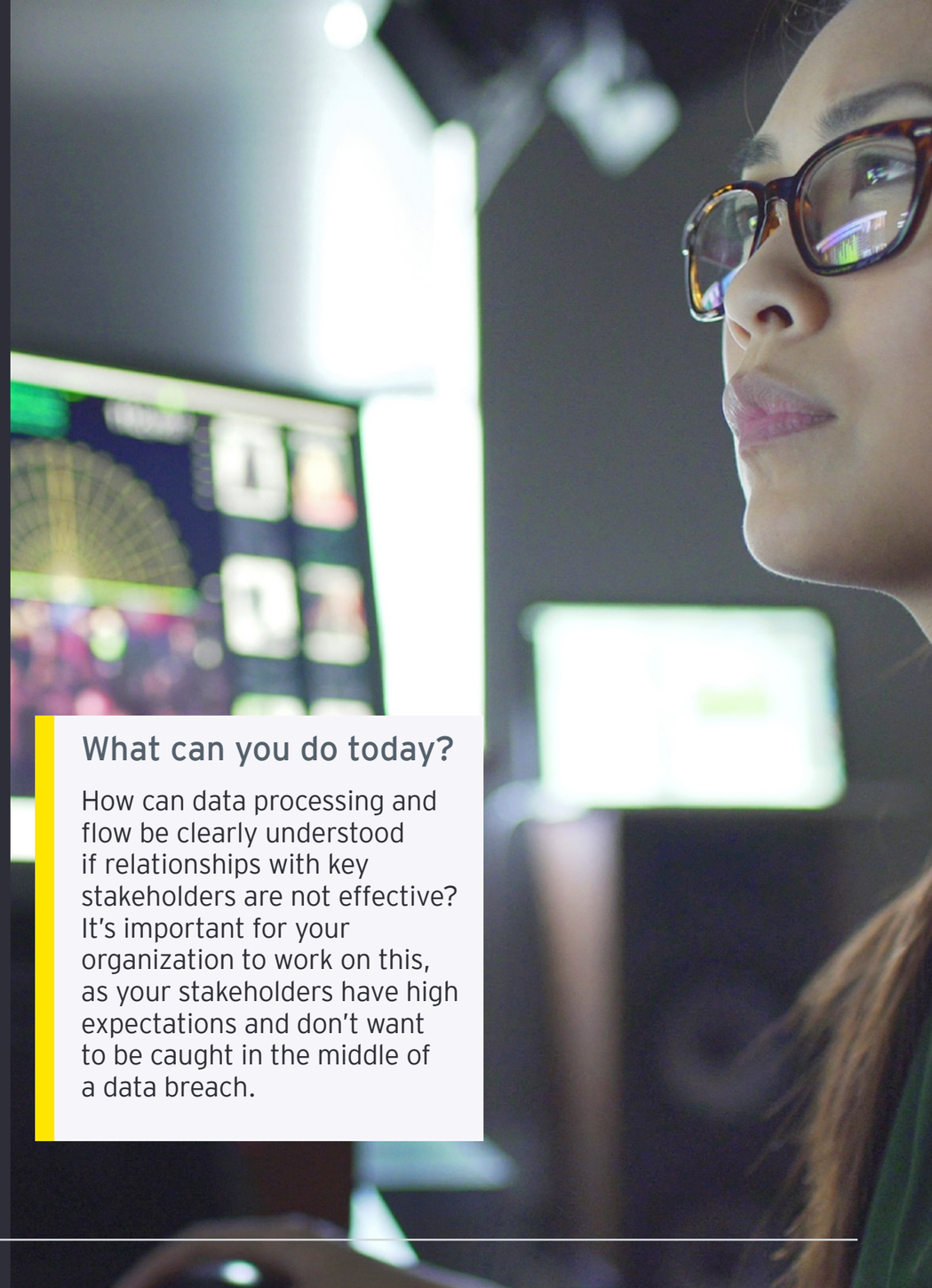
of respondents are concerned about high-profile data breaches such as those that have taken place in the technology, aviation and hospitality industries

43%

of respondents consider the COVID-19 pandemic to be a major driver of privacy

24%

of respondents report regulatory changes as a significant driver of privacy



What can you do today?

How can data processing and flow be clearly understood if relationships with key stakeholders are not effective? It's important for your organization to work on this, as your stakeholders have high expectations and don't want to be caught in the middle of a data breach.

2 Be kind, think human

Having a stakeholder-based approach means bringing the individual to the centre of the conversation and, by doing so, generating trust. Organizations that practice data trust are more apt to gain consumer trust, which in turn contributes to brand trust.

A successful privacy program should look beyond compliance to value generation. This creation – or preservation – of value should be translated into an increased trust in your relationships with all key stakeholders.

What are the top three considerations consumers have in mind when sharing personal information with an organization?

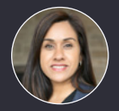
63%
of respondents want secure personal information collection and storage

57%
of respondents are looking for control over what personal information is shared

51%
of respondents seek trust in the company that's collecting their personal data

50% of consumers say that the COVID-19 pandemic has made them more willing to share their personal data if they know it is contributing to the research effort and/or community wellness. This demonstrates that by creating trust, consumers can be more open to data sharing. They just need to clearly see and understand the benefits.

> Organizations that want to reap the significant economic and social benefits of data need to create a data trust strategy that goes beyond compliance. The strategy must combine legal reform with the encouragement of new business models premised on consumer empowerment and supported by a personal information ecosystem.



Roobi Alam,
Privacy & Data Trust Leader, EY

COVID-19 has deeply transformed consumers' behaviours. It's not only that people are now working and studying from home full time – family life has changed, entertainment is different now, and social interaction outside the household has become more virtual than physical. These new ways might not be permanent, but this calibre of change in the game rules has set a precedent for the definition of the next normal.

As mentioned above, for what comes next, consumers expect organizations to be kind and think human. This comes largely from a Gen Z perspective. We conducted an analysis of what the oldest Gen Z cohort – those between the ages of 18 and 23, the largest generational cohort in history – thinks about this transformation. We found they expect the corporate world to stop focusing solely on profit and start recognizing that business should be more about people – caring for the environment, doing the right thing and putting individuals at the centre of the conversation. These concerns are among the ingredients needed to create trust and they are intimately connected with giving individuals controls on how their personal information is used.

What can you do today?

Overall, enabling individuals to take control over their identity and managing the ethical implications of data use will become a market differentiator for organizations. While some may choose minimum compliance to privacy legislation like the EU GDPR and the upcoming Bill C-11 in Canada or Bill 64 in Québec, forward-thinking organizations will shift their data trust strategy to enable methods of harnessing customer intention as opposed to simply reacting to customer behaviour.

3 Get support from enabling technology

It's hard, if not impossible, to think of generating data trust without technology. You might need some new tools to respond to this challenge. But before going there, you should be able to identify existing processes and tools you have for managing data so you can analyze which ones can help you generate data trust.

Our experience and ongoing research have helped us understand that there's always a way to better use resources to achieve the desired results. The EY Global Information Security Survey 2020 found the following examples:

14%

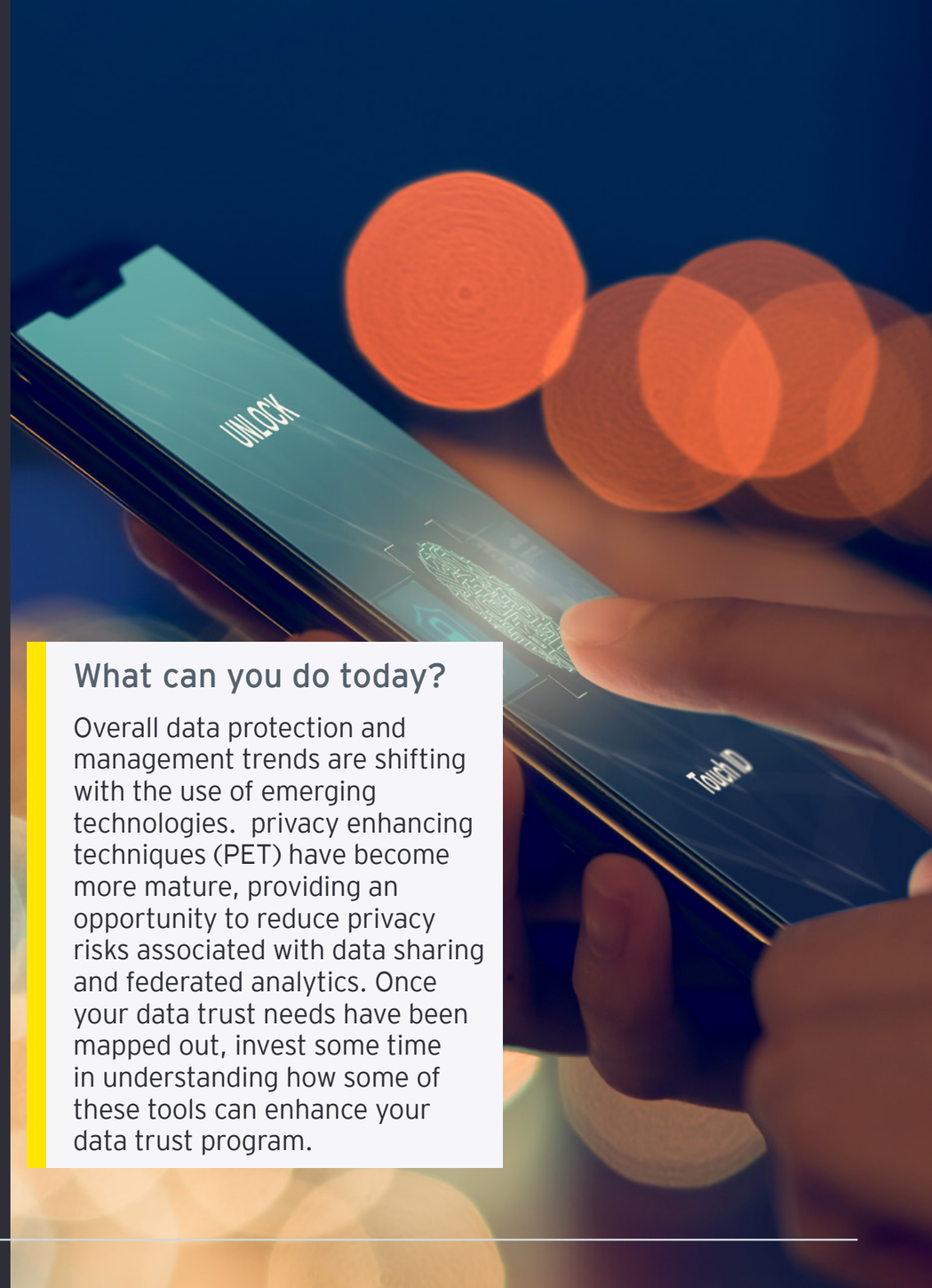
of new or increased cybersecurity funds are used on digital transformation programs, thus illustrating the lack of protection mechanisms in new initiatives

31%

of organizations engage in data protection only after designing processes or applications or never, meaning that data trust will not be generated

26%

of breaches were detected by the Security Operation Centre, the result of not effectively using technology already available



What can you do today?

Overall data protection and management trends are shifting with the use of emerging technologies. privacy enhancing techniques (PET) have become more mature, providing an opportunity to reduce privacy risks associated with data sharing and federated analytics. Once your data trust needs have been mapped out, invest some time in understanding how some of these tools can enhance your data trust program.

What does a data trust framework consist of?

Nearly **two thirds of Canadians (64%)** rated their knowledge of their privacy rights as **good or very good**.

Companies should seriously consider complying with privacy regulations since that's what people expect, and organizations could receive individual requests before they're expected.

More than **6 in 10** Canadians are confident that **government respects their privacy rights**, but fewer feel the same way about businesses.

The private sector needs to work on changing this perception to generate trust.

When it comes to trust Canadians have in specific types of businesses, **banks rate highest**.

Banks therefore need to keep on working on this to avoid negatively impacting trust, while other organizations need to define strategies to increase trust.

Canadians are concerned about how organizations will use their online personal information.

To generate trust, companies need to be clear and transparent in their privacy notices and effectively give control to individuals on how their personal information is used and disclosed.

Canadians are more likely to feel **uninformed about how businesses and governments handle their personal information**, and many feel they have little control over how their information is used.

Again, privacy notices need to be clear and offer easy-to-follow mechanisms for individuals to exercise their privacy rights. In addition, organizations should consider including privacy in their ESG reports to demonstrate their commitment.

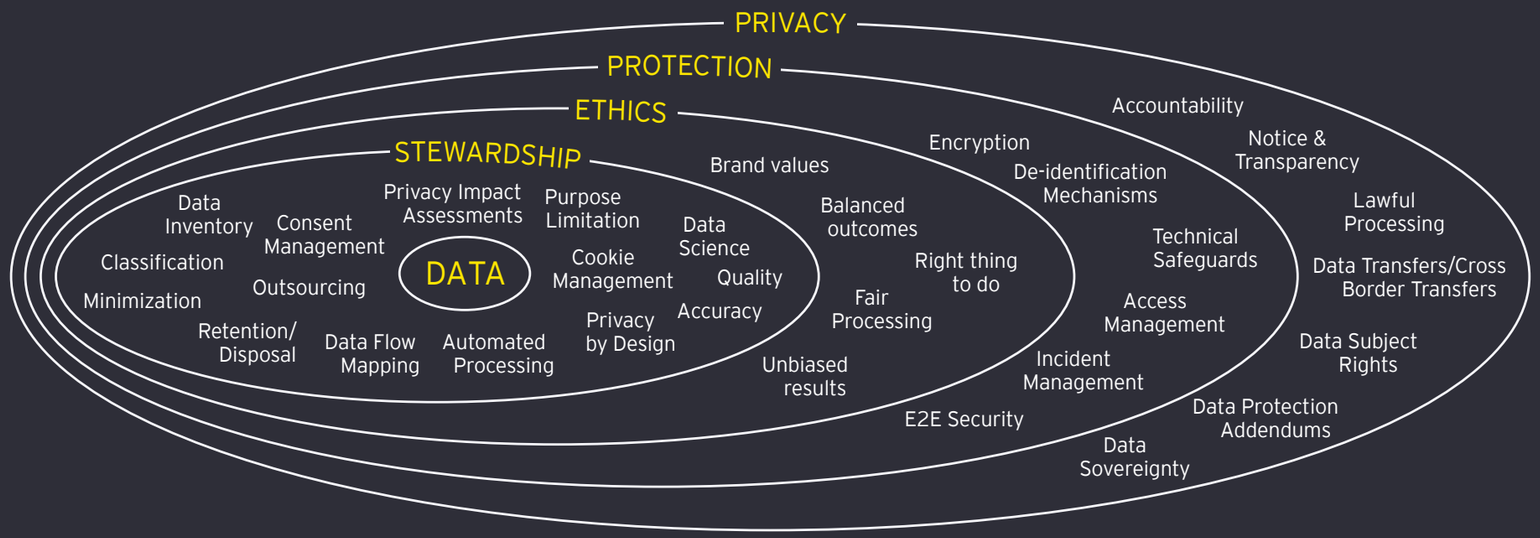
As this diagram illustrates, the creation of trust starts at inception with a solid data stewardship that sets the foundations for effective data management.

The next layer is a well-defined and thought-out data ethics model that properly reflects and operationalizes brand values. This layer is then reinforced through the enablement of the data protection mechanisms that respond to identified risk considerations.

The model is finally closed with the definition of an effective privacy program that should share data privacy accountability across the organization so that every single collaborator brings the individual at the centre of the conversation to effectively generate value and data trust.

This new strategy is important because it changes the focus of who benefits from the collection and use of personal information from businesses to consumers. It also increases consumers' trust by giving them control over how their data is collected and used while organizations still benefit from the use of big data and analytics.

The diagram below illustrates EY's vision for the generation of data trust.



DATA STEWARDSHIP + DATA ETHICS + DATA PROTECTION + DATA PRIVACY = **DATA TRUST**

"EY has gone to great lengths to embed privacy into their data trust by design. Enabling access to data via EY's data trust provides an invaluable service, leading with privacy being strongly protected: win-win.

Dr. Ann Cavoukian, Ph.D.
Executive Director, Global Privacy & Security by Design Centre

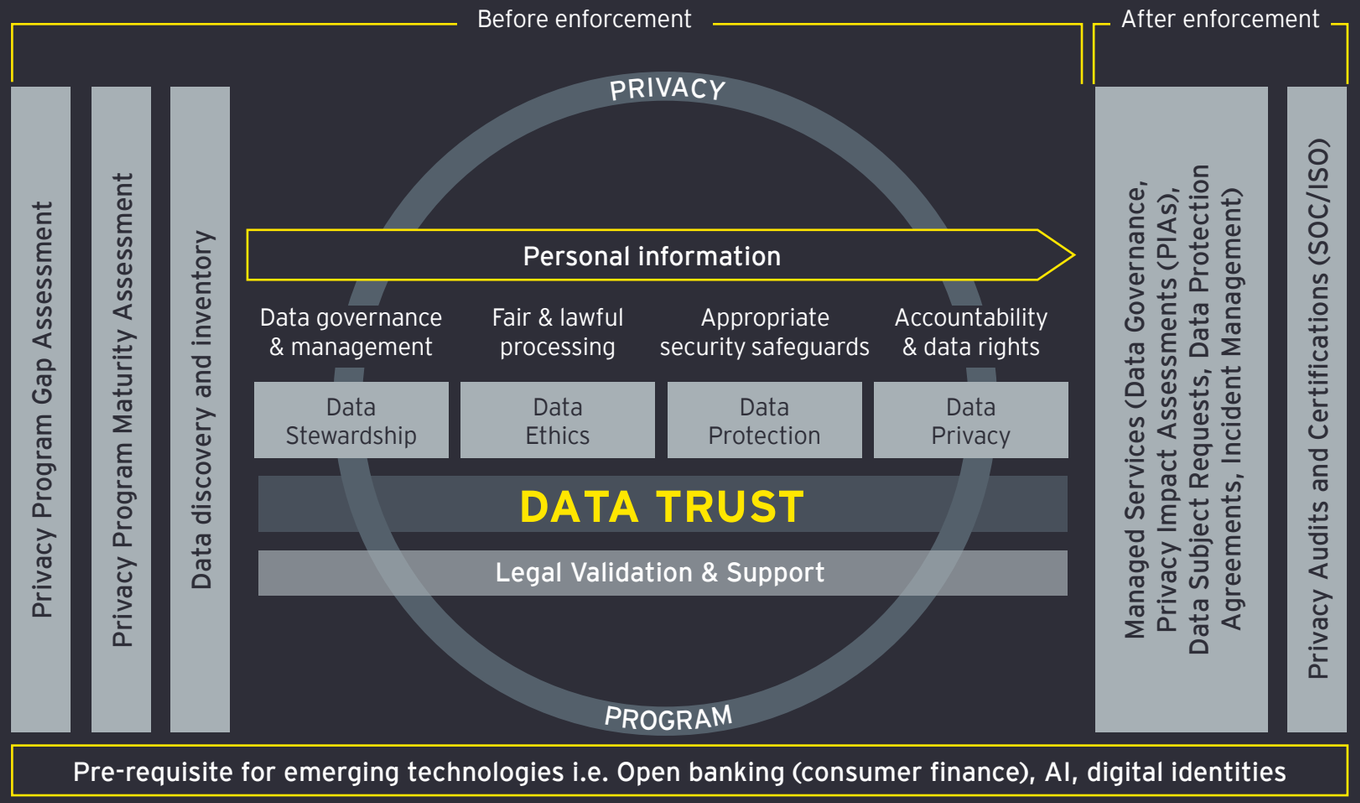
How EY can help

We can help you look beyond basic compliance. We execute our Data Trust services in a phased approach help you build a robust data trust program.

To achieve privacy compliance and support value generation for stakeholders, data trust requirements need to be embedded throughout the organization from a people, process and technology perspective.

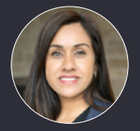
We bring significant experience in helping organizations meet their privacy and data trust needs. We can help you embed data privacy into your day-to-day activities using existing and emerging tools and support your value generation and compliance efforts across your organization.

- Multi-disciplinary by integrating the legal, IT, risk and business perspectives of privacy.
- Single EY Legal & Advisory Privacy offering to translate legal requirements into a risk-based, customized approach.
- Identification of pragmatic implementation options for privacy regulation readiness with minimal operational impact.
- Proven success in roll-out in multiple sectors and countries, with EMEIA reach and connectivity to other jurisdictions.



EY's Data Trust Framework not only complies with privacy regulations around the world, it helps organizations convert their data risk into data trust by looking for value generation beyond compliance. In addition, it is a pre-requisite for other emerging technologies such as open banking (consumer Finance), AI and digital identities.

To explore how our team can help you build meaningful data trust, contact a member of our team:



Roobi Alam
Privacy & Data Trust Leader
roobi.alam@ca.ey.com
+1 416 943 3284

Carlos Chalico
Privacy & Data Trust Senior Manager
carlos.perez.chalico@ca.ey.com
+1 416 943 5338

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

3787529
ED 00

ey.com/ca