Privacy and data protection

Challenges
Privacy has become a global business concern due to increasing regulatory requirements and greater public awareness of how personal information is being handled. In the digital economy, businesses are increasingly looking to monetise data and provide custom experiences while balancing their customers and users rights and expectations on how their personal information will be used. This operational and strategic tension requires a holistic and pragmatic approach to effectively manage privacy.

How Deloitte can help
Deloitte works with clients to answer questions that matter the most, such as: how to use personal information more effectively, how to demonstrate effective compliance, how to manage breaches and notifications, how to embed privacy capability and most importantly, how to best protect your customers privacy. Deloitte offers a tested and comprehensive suite of end-to-end privacy services and solutions to help you transform and maintain your management of regulatory, technology and operational challenges, enabling you to make the most of personal information and reduce privacy risk.

Key solutions

Privacy Strategy and Transformation Program
Privacy Operating Model
Data Discovery
Privacy Training, Awareness and Cultural Change
Preference Management and Customer Engagement
Customer Breach Support and Response

Processes and organisation
Review and implement the correct business processes and privacy operating model

Legal and compliance
Install privacy controls as part of unified risk management

Data management
Implement integrated and sustainable controls for personal data

Cyber security and IT
Implement the right technology and cyber governance measures

Contacts

Manish Sehgal
Asia Pacific and India
+91 9818 544 900
masehgal@deloitte.com

Anu Nayar
New Zealand
+64 2 1207 9573
anayar@deloitte.co.nz

David Batch
Australia
+61 2 8260 4122
dbatch@deloitte.com.au

Young Soo Seo
South Korea
+82 2 6676 1929
youngseo@deloitte.com

Frank Xiao
China and Hong Kong
+86 108 512 5858
franxiao@deloitte.com.cn

Haruhito Kitano
Japan
+81 80 3591 6426
haruhito.kitano@tohmatsu.co.jp

Anna Marie Pabellon
Southeast Asia
+63 2 581 9038
apabellon@deloitte.com

Chia-Han Wu
Taiwan
+886 2 4051 6888
chiahwu@deloitte.com.tw
OneTrust
Privacy Management Software

The World’s Most Widely Used Software
For Privacy, Security & Third-Party Risk Compliance

CCPA | GDPR | GLOBAL PRIVACY LAWS

- Privacy Program Management
- Privacy & Marketing User Experience
- Vendor Risk Management
- Incident & Breach Response

See How Over 3,000 Companies, Both Big and Small, Operationalize Compliance with OneTrust.

Visit Our Booth for a Demo!

JOIN US FOR A SESSION

FIRST SESSION
DATE: MON, 15 JULY
TIME: 11:00 - 12:15

GDPR (1 Year Later): Lessons From Data Breach Victims and Security Professionals
Speakers:
- Dorothy Chau, CIPP/A, CIPP/E, CIPM, FIP, Senior Lecturer, Hong Kong Baptist University
- Moderator: Jason Wai King Lau, CIPP/E, CIPM, FIP, Regional Leader, Hong Kong, IAPP; CISO, Crypto.com
- Rob Roe, Managing Director ANZ, OneTrust
- Scott Carlson, Head of Blockchain Security, Kudelski Security Chung Kei

SECOND SESSION
DATE: MON, 15 JULY
TIME: 13:30 - 14:30

Are Suppliers Your Biggest Data Breach Risk? Managing Third Party Vendor Risk
Speakers:
- Brendan Pat, CIPP/E, Data Governance Officer and Senior Data Counsel, Agoda
- Moderator: Rob Roe, Managing Director ANZ, OneTrust
- Wijaya Abori, CIPP/A, CIPM, Regional Data Protection Officer, Grab, FIP certification
Data security & privacy on Google Cloud Platform & G Suite

We create trust through transparency

Google Cloud offers detailed data processing and security related terms that describe our commitment to protecting your data. These terms, which are available for you to review on our website, reflect the following important commitments:

- We implement and maintain state-of-the-art technical and organizational measures to protect customer data.
- We notify customers promptly if we become aware of a security incident.
- We only process customer data in accordance with our customers’ instructions.

GCP Data Processing and Security Terms: cloud.google.com/terms/data-processing-terms
G Suite Data Processing Terms: gsuite.google.com/terms/dpa_terms.html

We are your trusted partner in security. We created and abide by five trust principles that guide our end-to-end security model so you can:

1. Know that your security comes first in everything we do

   - Purpose-built infrastructure:
     In designing and controlling chips, servers, and software used in our infrastructure, we can quickly develop and roll out a fix if a vulnerability is found. Reducing "vendor in the middle" risk allows us to minimize exposure for both ourselves and our customers.
     cloud.google.com/security/infrastructure

   - Encryption by default:
     Google encrypts all data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google. Google Cloud Platform encrypts customer data stored at rest by default, with no additional action required from you.
     cloud.google.com/security/encryption-in-transit cloud.google.com/security/encryption-at-rest

2. Control what happens to your data

   We process your business’s data according to your instructions. You can access your data when you want and take out the data you put in.

   Use our ever-expanding set of security tools and services across our product portfolio to help meet your policy, regulatory, and business objectives. Our current offerings span infrastructure security, network security, security monitoring and operations, endpoint security, data security, identity and access management, and application security.
   cloud.google.com/security/products

3. Depend on Google’s independently-verified security & privacy practices

   Independent auditors certify and validate our adherence to recognized international security and privacy standards. We’re constantly working to achieve additional certifications against global standards to earn your trust.
   cloud.google.com/security/compliance

4. Trust that we never give any government entity “backdoor” access to your data or to our servers storing your data

   When we receive requests for data from law enforcement agencies, our team rejects requests that are invalid and pushes back when requests are overly broad. We work hard to inform businesses about these requests as soon as we can, barring emergency circumstances or where we are prohibited by the legal nature of the request.

   We publish the locations of our data centers. They are highly available, resilient, and secure.
   cloud.google.com/about/locations

   Forrester

   cloud.google.com/analyst-reports

Learn more about Google Cloud regional and global infrastructure:
cloud.google.com/about/locations

Learn more about our Data deletion on GCP:
cloud.google.com/security/deletion

Learn more about Google Cloud for security:
cloud.google.com/security/govt-requests

Learn more about Google Cloud for data centers:
cloud.google.com/about/locations

Learn more about how Google protects the privacy of business’s data at privacy.google.com/businesses
Minimise Time to Compliance

Choose Nymity’s Expert Privacy Platform for the GDPR, CCPA, LGPD, and the World’s Privacy Requirements

GET STARTED @ WWW.NYMITY.COM
Complexity. We untangle it.

The volume and density of law relating to cross-border financial services activities is overwhelming. Add to this the spiralling costs of commissioning legal surveys which quickly become outdated, and it's easy to see the value of aosphere's online legal solutions.

Rulefinder Cross Border Data Transfer is an online legal database, enabling firms to overcome barriers to cross-border data transfers:

– covers data protection, confidentiality and outsourcing laws for 60+ jurisdictions
– analysis of EU GDPR requirements
– colour-coded summaries
– detailed legal memorandum from leading local counsel
– factsheets detail how to implement key compliance requirements
– compare and version control/blacklines of updates
– email alerting service
– annual subscription fee

Visit aosphere.com/aos/cbd to request a free trial

Visit the aosphere stand to find out more
Review and compare regulations across multiple jurisdictions at a glance.

Cross-Border Charts help you to easily research and compare data protection requirements globally. Each country and topic is supported by specific Guidance Notes, to provide you with an in-depth analysis of the applicable requirements.

Cross-Border Charts are available on key areas such as:

Access all Cross-Border Charts HERE
Manage Compliance for GDPR, CSL, PDPA, and Other Privacy Regulations

TrustArc Privacy Compliance Solutions

Privacy Platform
- Data Flow Manager
- Assessment Manager
- Cookie Consent Manager
- Website Monitoring Manager
- Direct Marketing Consent Manager
- Individual Rights Manager
- Ads Compliance Manager

Privacy Consulting & Training
- Compliance Assessments
- Vendor Risk Management
- DPIA / PIA Program Development
- Breach Response Plans
- Policies and Procedures
- GDPR and CCPA Implementation
- Employee Privacy Training

Privacy Certifications
- GDPR Validation
- EU Privacy Shield Verification
- APEC CBPR and PRP Certification
- Children's / COPPA Certification
- TRUSTe Enterprise Certification
- EDAA Certification
- Dispute Resolution Service

www.trustarc.com | 888-878-7870 | contact-sales@trustarc.com