Global Trends in Privacy

Exploring how global regulatory changes are impacting the way organizations do business
Your PwC facilitators

Michael Spadea
Privacy Managing Director

- Founded and led the U.S. privacy practice for an international consulting firm
- Oversaw information governance for enterprise customers in Microsoft’s Services division
- Served in London as global privacy counsel for the Barclays Banking Group, and Head of Privacy for its Wealth Advisory division
- Performed GDPR readiness assessments for financial institutions, a technology service provider, and an online media and advertising platform; provided tactical guidance, strategic roadmaps, and governance
- Conducted GLBA privacy and security assessments and testing for financial institutions resulting in regulators closing findings

Matthew Reinke
TMT Director

- 22 years of experience providing internal audit services, governance, risk, compliance (GRC) services, consulting, and external audit services to a wide range of companies
- Served in various leadership capacities building service capabilities, managing and reporting on the growth of our service lines, and staff development
- Assisted global companies in developing strategies, methodologies and procedures for Internal Audit departments, establishing and running SOX programs, GRC programs, Ethics & Compliance programs, and various finance effectiveness capabilities
- Leads PwC’s Seattle’s internal audit services for ISO 27001 and privacy engagements
- President of the Puget Sound IIA Chapter, and an Adjunct Professor in Accounting at UW-Bothell
Agenda

- Regulatory trends
- Industry trends
- Evolving privacy programs
- Considerations for Internal Audit
- Appendix
Regulatory trends
Global privacy outlook

A variety of new global privacy regulations will soon require organizations to focus on user data and provide transparency in how they’re collecting, sharing, and using such data.
Overarching regulatory trends

Given the variety of data protection regulation around the world, companies need to approach privacy in a more holistic manner. Designing programs around these four areas of compliance will help organizations reach a defensible level of compliance with most regulations, and allow flexibility in right-sizing for particular laws, as needed.

**Data Collection & Access**
- Personal information collection
- Processing and handling by data controllers
- International data transfers
- Sensitive personal data
- Employee personal data
- Server location and data localization

**Data Processing**
- Sectoral vs. Omnibus laws
- Jurisdiction and territoriality
- Data security breaches and required notifications
- Data retention obligations
- Online tracking and advertising

**Third Parties**
- Vendor agreements and mandatory assurances
- Security requirements

*Companies are refocusing the customer experience to enhance trust by demonstrating a commitment to privacy and the protection of personal data.*

**Individual Rights**
- Data subject consent
- Notice and disclosure requirements
- DPO and other privacy program requirements
- Enforcement and sanctions
### Spotlight: EU & EEA

**Regulations:** General Data Protection Regulation (GDPR), ePrivacy Regulation

#### GDPR

- GDPR was intended to **harmonize EU data protection regulatory landscape**, including establishing a one-stop shop lead data protection authority
- Strict rules regarding lawful basis for processing personal data
- **Mandatory data breach notification** – notice to regulators and data subjects within 72 hours
- Imposes security **obligations on processors** of personal data

#### ePrivacy Regulation

- **Broadens the scope of the current ePrivacy Directive** and aligns the various online privacy rules that exist across EU member states.
- The regulation takes on board all definitions of privacy and data that were introduced within GDPR, and acts to **clarify and enhance** it.
- **Larger compliance gaps** exist in organizational readiness for the ePrivacy Regulation than for GDPR
- Requires organizations to understand its use of personal data in **marketing**, use of **cookies**, and any other data handling measures resulting out of **machine-to-machine communications**
Spotlight: Russia

**Regulations: Data Localization Law**

- Data operators processing personal data of Russian citizens, whether collected online or offline, are obliged to record, systematize, accumulate, store, update, change and retrieve such data in databases located within the territory of the Russian Federation.
  - Applies to Russia-based data operators, including subsidiaries and representative offices of foreign companies.

- Literal wording of the law does not explicitly require data operators to perform data processing operations solely within the territory, it just requires that a copy of the data be stored in Russia.

- No explicit prohibition of cross-border transfers.

- No individual right of action.

- Data operators that violate the law will be added to a register of personal data violators and access to the operators’ may be restricted.
Background:

- **Stated purpose:** “APEC economies recognize the importance of protecting information privacy and maintaining information flows among economies in the Asia Pacific region and among their trading partners. . . The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent member economies from gaining all of the benefits of electronic commerce.”

- A **flexible framework**, rather than a directive
Spotlight: China

**Regulations:** China Cybersecurity Law (CSL)

- China’s **first comprehensive law** on cybersecurity
- Data classified as “personal data” and “important data” which generally relates to **any information** the government may deem important for national security purposes
- **Applicable to anyone** owning or operating a computer system network (“critical information infrastructure (CII) operators”), and suppliers of network products and services (“network operators”)
- Data collected in China must be **stored in China**
- Penalties divided by **monetary, criminal and operational** violations, including fines between $1,500 - 75,000, for each violation
Spotlight: India

**Regulations:** Personal Data Protection Bill (2018)

- Bill was introduced following Supreme Court’s declaration of **privacy as a fundamental human right**
- Three key approaches:
  - Sectoral (similar to US)
  - Omnibus (similar to EU)
  - National security (similar to China)
- “**Data Principals**” have rights similar to those under GDPR
- “**Data Fiduciaries**” are Indian entities, or carry out data activities in India; they must store at least 1 copy of personal data on servers in India
- Periodic data audits (new to India)
- Failure to respond to **data subject requests:** $70/day per request (ceiling of $13,540)
- **General fines:** $728,000, or 2% global annual turnover of the preceding financial year, whichever is higher
Spotlight: Canada

**Regulations**: PIPEDA (2018 update), Canadian Anti-Spam Law (CASL)

**PIPEDA**
- 2018 amendment to PIPEDA entitled *Breach of Security Safeguards* requires private companies in Canada that collect, use or disclose personal information to comply with **new rules for data breach record-keeping and notifications**
  - Notifications to:
    - The Office of the Privacy Commissioner (OPC)
    - Affected individuals
    - Other organizations
  - Private organizations will now also have to **maintain a record of all security incidents** involving personal data for 24 months after the date the breach is confirmed. Penalties for improper record-keeping can be up to $100,000

**CASL**
- Requires **consent** to send commercial electronic messages to an email account, telephone account or instant messaging account
- Applies to **any computer system in Canada** used to send CEMs
- Messages must include a compliant **unsubscribe** process
- Fines up to $10 million
- Private right of action was to be allowed beginning July 2017 (maximum $1 million per day in violation), but this provision of the law was **recently suspended** and is not in effect
The rapidly evolving US regulatory landscape

Companies are refocusing the customer experience to **enhance trust** by demonstrating a commitment to privacy and the protection of personal data.

**Proposed federal regulations range from general guiding principles that override many state regulations to complex laws with harsh criminal penalties that leave in place state laws.**

- **August 28, 2017**
  - The Consumer Right to Privacy Act is filed and proposed as a November 2018 election ballot measure

- **June 22, 2018**
  - Leaders of the initiative agree to withdraw their ballot measure in exchange for the passage of the California Consumer Privacy Act by June 29, 2018

- **February 22, 2019**
  - CCPA amendment (SB-561) proposes to expand private right of action for any violation, and remove the 30-day cure period for actions brought by the AGO

- **May 2, 2018**
  - Supporters collect and file 625,000 signatures—nearly double the number required to qualify the measure on the November 2018 ballot

- **June 28, 2018**
  - The Legislature passes the California Consumer Privacy Act unanimously and the bill is signed into law

- **January 1, 2020**
  - The CCPA goes into effect

**Washington: SB-5376 has just passed in the Senate, and will go to the House for consideration. The bill includes similar data subject rights to GDPR, and also regulates facial recognition and consumer profiling.**

**California: CCPA**
- Requires covered companies to develop written policies for the destruction and disposal of documents containing personal information.
- Requires an opt-out of data selling, defined broadly.

**Colorado: HB18-1128**
- Requires covered companies to develop written policies for the destruction and disposal of documents containing personal information.

**Illinois: BIPA regulates the collection and use of biometric data.**

**New York: Under DFS cyber regulations, entities must file a cybersecurity regulation Certification of Compliance.**

**South Carolina: H4655 requires insurance companies to develop written cybersecurity programs and incident response plans.**
PwC’s Comparison of Key GDPR and CCPA Requirements

Similar to the GDPR, the CCPA will require organizations to focus on user data and provide transparency in how they’re collecting, sharing, and using such data. But to what extent can a company extend its GDPR capabilities into its California operations to prepare for CCPA? Certain CCPA requirements overlap with the existing GDPR individual rights requirements, which may give GDPR-ready organizations a jump start on building a capability around user-data handling practices.

<table>
<thead>
<tr>
<th></th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>EU personal data processed</td>
<td>California residents’ personal data collected</td>
</tr>
<tr>
<td><strong>Right to access</strong></td>
<td>Right to access all EU personal data processed</td>
<td>Right to access California personal data collected in last 12 months, delineated between sold and transferred</td>
</tr>
<tr>
<td><strong>Right to portability</strong></td>
<td>Must export and import certain EU personal data in a user-friendly format</td>
<td>All access requests must be exported in user-friendly format, but there is no import requirement</td>
</tr>
<tr>
<td><strong>Right to correction</strong></td>
<td>Right to correct errors in EU personal data processed</td>
<td>Not included in CCPA</td>
</tr>
<tr>
<td><strong>Right to stop processing</strong></td>
<td>Right to withdraw consent or otherwise stop processing of EU personal data</td>
<td>Right to opt-out of selling personal data only; must include opt-out link on website</td>
</tr>
<tr>
<td><strong>Right to stop automated decision-making</strong></td>
<td>Right to require a human to make decisions that have a legal effect</td>
<td>Not included in CCPA</td>
</tr>
<tr>
<td><strong>Right to stop third-party transfer</strong></td>
<td>Right to withdraw consent for data transfers involving second purposes of special categories of data</td>
<td>Right to opt-out of selling personal data to third parties</td>
</tr>
<tr>
<td><strong>Right to erasure</strong></td>
<td>Right to erase EU personal data, under certain conditions</td>
<td>≃ Right to erase personal data collected, under certain conditions</td>
</tr>
<tr>
<td><strong>Right to equal services and price</strong></td>
<td>At most, implicitly required</td>
<td>Explicitly required</td>
</tr>
<tr>
<td><strong>Private right of action damages</strong></td>
<td>No floor or ceiling</td>
<td>No floor or ceiling on actual damages</td>
</tr>
<tr>
<td><strong>Regulator enforcement penalties</strong></td>
<td>Ceiling of 4% of global annual revenues</td>
<td>No ceiling - $7,500 per intentional violation</td>
</tr>
</tbody>
</table>

Narrower  | Broader  | Similar  | Absent
## CCPA vs GDPR (1 of 2)

<table>
<thead>
<tr>
<th>What is data processing?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Any operations performed on personal data, automated or otherwise.</td>
<td>● Any operations performed on personal data, automated or otherwise.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whose information is protected?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>● <strong>Natural persons</strong> (also known as data subjects) in the <strong>European Union</strong> who can be identified, directly or indirectly, by reference to an identifier.</td>
<td>● <strong>Consumers</strong>, which are natural persons who are <strong>California residents</strong> (per Section 17014 of Title 18 of the California Code of Regulations).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who must comply?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>● “Controllers” and “processors” that process <strong>personal data of data subjects within the European Union</strong>, regardless of whether the processing takes place in the Union.</td>
<td>● Businesses that do business in California and that collect consumers' personal information, or authorize another to collect, that <strong>meet at least one</strong> of the following: ○ Annual gross revenues are equal to or greater than $25m ○ Buys/receives, or shares/sells personal information of more than 50,000 consumers ○ 50% of annual revenue from selling consumer personal information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When can data be processed?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Specific <strong>lawful basis</strong>, including: consent, performance of a contract, to protect a person’s vital interests, for the public interest, legitimate interests</td>
<td>● <strong>No specific bases</strong> for processing <strong>Sale of consumer information is prohibited</strong> if a consumer has <strong>opted out.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What rights do data subjects have?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Right to be informed of data processing practices</td>
<td>● Right of data access</td>
<td></td>
</tr>
<tr>
<td>● Right to access to personal data and other information about processing</td>
<td>● Right of data erasure</td>
<td></td>
</tr>
<tr>
<td>● Right to rectification</td>
<td>● Right to stop data selling and disclosure</td>
<td></td>
</tr>
<tr>
<td>● Right to be forgotten</td>
<td>● Right to equal service and price, even if privacy rights are exercised</td>
<td></td>
</tr>
<tr>
<td>● Right to restrict processing</td>
<td>● Right to stop third party transfer</td>
<td></td>
</tr>
<tr>
<td>● Right to data portability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Right to object to processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Right not to be subject to a decision based solely on automatic processing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### CCPA vs GDPR (2 of 2)

<table>
<thead>
<tr>
<th>How do the laws apply to children’s data?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Under age 16, requires parental consent is required (individual member states may lower age to 13).</td>
<td></td>
<td>• Businesses cannot knowingly sell data of consumers younger than 16 unless the consumer has opted in to the sale (if the consumer is between 13 and 16), or the parent or guardian has opted in to the sale (if the child is under 13).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What are the exemptions?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Processing by legal authorities in relation to investigating, detecting, or prosecuting criminal offenses or penalties; processing for journalistic, academic, or literary expression purposes; limited exemptions for processing for scientific, historical research, or archiving purposes in the public interest; processing for purely personal or household activities.</td>
<td></td>
<td>• Processing for compliance with federal state or local laws, including, but not limited to, GLBA and HIPAA, or legal investigations; collection or sale of de-identified or aggregate consumer information; collection or sale of personal information that takes place wholly outside of California; sale of information to consumer reporting agencies for a consumer report; where compliance would violate evidentiary privilege.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Do consumers have a private cause of action?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Yes</td>
<td></td>
<td>• Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What fines can be levied?</th>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 20M EUR or up to 4% of total global revenue of the previous year.</td>
<td></td>
<td>• Private causes of action, between $100 and $750 per consumer per incident, or actual damages, whichever is greater. • For California AG actions, civil penalties of up to $7,500 per intentional violation</td>
</tr>
</tbody>
</table>
What’s the risk of non-compliance?

- **Regulatory risk**
  - Fines and penalties
  - Data protection audits (can last several decades)
  - Exclusion from trade associations or alliances

- **Financial risk**
  - Loss of revenue
  - Litigation costs (including shareholder lawsuits, class actions or individual private action)
  - Civil and/or criminal penalties for data breaches
  - Remediation costs

- **Reputational risk**
  - Brand damage
  - Loss of consumer trust
  - Loss of employee trust
  - Loss of patient trust
  - Consumer attrition

- **Operational risk**
  - Restricted operations
  - Invalidated data sharing or selling
  - Incident response remediation

For example, a breach affecting 50 million users could result in the following fines:
- **GDPR**: over $1.63 billion
- **Brazil Data Protection Act**: over $815 million
- **FTC**: fines upward of $500 million may be levied, based on FTC trends
- ...and **many more**, for global companies!

**US education technology company** privacy rights activism caused fatal reputational damage to the education data company, causing it to shutdown in 2014.

**Global social media technology company**: Since prominent data misuse scandal in 2018, 44% of Americans between 18-27 years old have deleted the application from their devices.
Industry trends
Growing consumer awareness of privacy is raising concerns beyond legal repercussions to public perception and brand reputation. Companies are beginning to highlight how they protect your data and empower customers and employees to set their own privacy preferences.

“How important is it to you, personally, that companies work to truly make a positive difference?”

Privacy as a differentiator

2018 Societal ROI. Harris Insights & Analytics. A Stagwell Company LLC 2018
Technology impacts on privacy

There is a shift underway to a more strategic, risk-based view of privacy. With the growing value and risks associated with data, a new risk class is emerging; “Reticence risk” is the lack of structured risk-driven decision making that sub-optimizes value of data.

**From**

Traditional processes and structures that are focused on regulatory risk and compliance requirements

**To**

Ethical data stewardship programs that minimize risk and support the digital strategy through data optimization

---

**Companies are adopting advanced authentication technologies**

<table>
<thead>
<tr>
<th>Technology Type</th>
<th>AI Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>60%</td>
</tr>
<tr>
<td>Software tokens</td>
<td>59%</td>
</tr>
<tr>
<td>Hardware tokens</td>
<td>55%</td>
</tr>
<tr>
<td>Cryptographic keys</td>
<td>53%</td>
</tr>
<tr>
<td>Multifactor authentication</td>
<td>51%</td>
</tr>
<tr>
<td>National IDs and ePassports</td>
<td>50%</td>
</tr>
<tr>
<td>Smartphone tokens</td>
<td>48%</td>
</tr>
<tr>
<td>Other</td>
<td>20%</td>
</tr>
</tbody>
</table>


---

**AI Impact on Components of a Privacy Program**

- Privacy by design
- Individual rights
- Data lifecycle management
- Cross-border data transfer
- Data processor accountability
- Incident management
- Information security
- Training & awareness
- Strategy & governance
- Policy management

AI Impact on Components of a Privacy Program

Highest

Lowest
Evolving privacy programs
Privacy affects more than the privacy office

Privacy Office
- Enhancing consumer notice and transparency
- Enforcing Privacy by Design
- Conducting Privacy Impact Assessments

Legal
- Evaluating legal compliance gaps
- Advising on updates and changes to the law
- Managing contract process with 3rd party sellers, buyers, and processors
- Driving data breach notification
- Managing response to enforcement actions, private and state

Compliance
- Administering corporate policies and procedures, including records retention
- Enforcing privacy requirements across the organization

Information Security (IS)
- Promoting security throughout the data lifecycle
- Assisting with data-breach notification
- Driving incident response
- Involved in response to civil and state enforcement actions

Information Technology (IT)
- Ensuring rights of access and deletion upon identity verification
- Enhancing data-lifecycle management functions
- Managing consent indicators and logs
- Maintaining inventory of systems and processing activities

Marketing and Human Resources (HR)
- Respecting opt-in and opt-out consent on a rolling basis
- Training employees on privacy compliance
- Limiting data collection and access as a best practice
- Maintain standards with 3rd party sellers, buyers or processors

Customer Service and Operations
- Ensuring rights of access and deletion
- Fielding questions, inquiries, concerns while maintaining brand reputation

Internal Audit
- Monitoring and reporting privacy program and compliance
- Promoting continued accountability
- Performing independent assessments of administrative, technical, and physical controls

Organizational Impact
The components of an effective privacy program

The following ten privacy domains will help organizations understand all the documents and processes required to achieve compliance with global privacy and data protection legislative and regulatory requirements.

1. **Strategy and governance**
   Define an overarching privacy program governance structure, roles, and responsibilities designed to coordinate, operate, and maintain the program on an ongoing basis.
   - Privacy Program Governance
   - Steering Committee Structure
   - Privacy Program Charter, KPIs
   - Privacy compliance controls framework

2. **Policy management**
   Privacy policies, notices, procedures, and guidelines are formally documented and consistent with applicable laws and regulations.
   - Privacy policy
   - Notice inventory and analysis matrix
   - Policy gap analysis document
   - Change management strategy

3. **Cross-border data transfer**
   Determine go-forward cross-border data transfer strategy based on current and future planned data collection, use, and sharing.
   - Cross-border mechanism assessment
   - Fitness assessment for alternative mechanisms (e.g. BCRs)
   - Updated vendor contract clauses and standard language (as needed)

4. **Data lifecycle management**
   Create ongoing mechanisms to identify new personal data processing and use activities and implement appropriate checkpoints and controls.
   - Data inventory and mapping
   - Personal data use governance mechanisms – legal basis analysis and documentation
   - Ongoing data inventory/mapping management and validation process

5. **Individual rights processing**
   Enable the effective processing of consent and data subject requests, such as data access, deletion, and portability.
   - Data subject rights decision matrix, process flows, user experience guidance
   - Procedures and tools to receive, evaluate, and execute requests
   - Consent management framework

6. **Privacy by design**
   Develop a strategy and playbook for Privacy by Design (PbD) to incorporate privacy controls and impact assessments throughout the data lifecycle for new and changing data use initiatives.
   - PbD strategy and implementation playbook
   - PbD socialization workshop collateral
   - PIA tools, templates, and workflow
   - PIA risk rating engine

7. **Information security**
   Identify existing security information protection controls and align security practices with regulatory considerations.
   - Security strategy assessment
   - Risk analysis
   - User access management process
   - Defined backup, disaster recovery, and business continuity process
   - Encryption strategy
   - Security risk framework

8. **Incident management**
   Align incident response processes with regulatory specifications and reporting requirements. Establish a triage approach to evaluating potential privacy.
   - Incident Response and Breach Plan
   - Playbooks for business units
   - Triage frameworks for notifying supervisory authorities and individuals
   - Assessment mechanism to determine harm to the individual

9. **Data processor accountability**
   Establish privacy requirements for third parties to mitigate risks associated with access to the organization’s information assets.
   - Inventory of third parties where personal data is transferred
   - Validation of data transfer mechanisms and associated contractual protections
   - Due diligence/assessment procedures
   - Risk ranking and ongoing monitoring plans for third parties

10. **Training and awareness**
    Define and implement a training and awareness strategy at the enterprise and role level.
    - Data privacy training and awareness strategy
    - List of roles/functional areas for targeted training
    - Privacy training collateral
Levels of accountability

Organizations are typically gearing up for GDPR across three pillars of accountability: policy, process, and practice. We’re observing Internal Audit start to own the third pillar, practice, in supporting the organization’s readiness activities.

### Three Levels of Readiness

<table>
<thead>
<tr>
<th>Policy</th>
<th>Process</th>
<th>Practice</th>
</tr>
</thead>
</table>
| • Defining how data is used within the business | • Implementation of policy and technology requirements to enable compliance:  
  - Data deletion technology;  
  - Data inventory and process flow maps;  
  - PIA/DPIA process deployed across key areas | • Developed framework and controls (security and privacy)  
• Program testing, e.g. Internal Audit testing over the program as implemented or through change |
| • Internal policies drafted and aligned with GDPR | | |
| • Process documents developed across the business | | |
| • Stakeholder socialization, and buy-in | | |

**Internal Audit Support**
Considerations for Internal Audit
PwC’s five-phased methodology you see below is meant to assess organizations’ current capabilities, design and implement program components, and then continually sustain privacy operations.

### Privacy program readiness lifecycle

**Assess current capabilities**
- **Discover & analyze**: Identify and classify relevant data, systems and processes, and assess organizational readiness for data strategy optimization.
- **Assess & recommend**: Assess privacy control readiness within the in-scope data boundary against existing capabilities.

**Design the future state**
- **Strategize & plan**: Mobilize cross-functional support and accountability for remediation and implementation.

**Operate and sustain**
- **Design & build**: Implement capabilities, mitigate identified gaps, and establish sustainable privacy controls.
- **Operate & monitor**: Establish ongoing compliance mechanisms to promote continued accountability.

### Privacy program implementation areas

- **Strategy and governance**
- **Policy management**
- **Cross-border data transfer**
- **Data lifecycle management**
- **Individual rights processing**
- **Privacy by design**
- **Information security**
- **Privacy incident management**
- **Data processor accountability**
- **Training and awareness**
Internal Audit and the privacy journey

Internal Audit can achieve sustained accountability and influence positive risk management outcomes by establishing repeatable internal audit practices to continuously evaluate the compliance posture of privacy requirements helping to continuously improve and mature an organization’s privacy program.

**Plan**
- Identify scope of audit, key focus areas, and develop test procedures and evidence request list for privacy controls

**Test**
- Test the design and operating effectiveness of controls across the ten privacy domains

**Validate remediation**
- Validate remediation by re-test of failed privacy controls

**Operate & monitor**
- Establish ongoing compliance mechanisms to promote continued accountability

**Drive remediation activities**
- Mitigate risk by driving remediation activities across the enterprise to strengthen the state of privacy compliance

**Identify gaps**
- Identify control design and execution gaps through testing and review of evidence

**Operate & sustain**
- Establish repeatable internal audit practices to continuously evaluate the compliance posture of privacy requirements helping to continuously improve and mature an organization’s privacy program.

**Policy management**
- Cross-border data transfer
- Data lifecycle management
- Individual rights processing
- Privacy by design

**Information security**
- Privacy incident management
- Data processor accountability
- Training and awareness
Objectives

Independently audit the organization’s current privacy and data protection capabilities against a privacy controls framework. Identify capability gaps across the ten privacy domains, capture management’s response, and develop corrective action plans tailored to organizational goals, objectives, and risk profile.

Privacy audit plan and design

- Perform discovery efforts to understand the organization’s operational environment related to privacy
- Develop a privacy controls framework across the ten privacy domains, inclusive of test procedures and evidence request list, tailored to the organization’s business model and personal data processing
- Identify internal audit respondents across the ten privacy domains to provide input into the privacy audit

Validate remediation

- Develop high level corrective action plans for capability gaps across the ten privacy domains tailored to the organization’s goals, risk profile, and current and planned personal data processing
- Debrief leadership and other key stakeholders on outcomes of the privacy audit

Test

- Review existing documentation related to current state of privacy compliance
- Validate execution of control activities through sample testing, where appropriate
- Document audit results describing the current state of the organization’s privacy compliance posture

Identify gaps

- Evaluate the organization’s current state against the privacy controls framework, and document audit findings in an audit report, including capability gaps

Drive remediation activities

- Assist with capturing management’s response to audit findings driving remediation accountability
Security for privacy

Both privacy and information security have roles to play in a comprehensive data protection strategy. It is commonly stated that you can have security without privacy, but that you cannot have privacy without security, as those controls are foundational. **Security for privacy** is the protection of personal data against unauthorized physical and logical access.

**Privacy** extends beyond information security to consider the entire lifecycle of personal data and the business processes that use it.

**Information Security** is a foundational set of services that every organization needs to implement to protect confidentiality, integrity, and availability.
Transforming information technology

**Policy management**
- External-facing policy management
- Internal-facing policy and procedure document management

**Data lifecycle management**
- Data use and ethics governance
- Data inventory, mapping, and classification
- Data loss prevention
- De-identification

**Privacy by design**
- Privacy impact assessments

**Incident management**
- Incident readiness and response
- Privacy attestation and breach response

**Training and awareness**
- New hire training
- Role-based training
- General awareness activities

**Cross-border data transfer**
- Global data transfer strategies

**Individual rights processing**
- Service management

**Information security**
- Identity and access management
- Database security
- Cloud security
- Cyber risk and governance
- Network security
- Vulnerability management

**Data processor accountability**
- Third party risk management
- Vendor security reviews

**Foundational support**
- Analytics tools and dashboards (risk and compliance, sales and marketing)
- HR operations
- Change management

Strategic insight and governance
- Privacy strategies for digital transformation
- Privacy compliance and monitoring
- Global privacy regulatory and maturity assessments

**Data management**
- Risk and compliance management
- Sales and marketing management

**HR operations**
- Change management
Appendix
A closer look – Our global privacy network and thought leadership

We have a global privacy network, with dedicated privacy resources working in over 40 countries delivering a range of privacy related services. In short, we can provide privacy expertise wherever you operate.

Broad network of experienced teams

PwC’s privacy program is led by experienced teams who tap into a broad network of resources. They help businesses conduct thorough risk assessments based on CCPA requirements, rethink data governance strategy, and help implement holistic data-privacy enhancements and compliance-monitoring processes.

2,900+ cybersecurity and privacy practitioners

Our 2,900+ practitioners include highly trained and specialized consultants, attorneys, auditors, technologists, and industry veterans with experience helping global businesses across industries.

PwC privacy thought leadership

CCPA
- America’s GDPR? Seven workstreams to implement California’s CCPA
- Your readiness roadmap for the California Consumer Privacy Act (CCPA)

Data Strategy
- Monetizing data while respecting privacy: How data-use governance can unlock business value and mitigate risk
- Responsibly leveraging data in the marketplace: Key elements of a leading approach to data-use governance
- What CEOs need to know about privacy ethics, economics and risks

GDPR
- US multinationals should develop an EU privacy regulator affairs strategy: 3 questions to consider
- Operational Impacts of the General Data Protection Regulation (GDPR)
- Data Breach Notification: 10 Ways GDPR Differs From the US Privacy Model
- Five critical success factors for effective GDPR data-protection impact assessments
- Five critical success factors for GDPR data subject rights
- Pulse Survey US Companies ramping up General Data Protection Regulation (GDPR) budgets

We are a global privacy thought leader at the heart of conversations that matter.
For more please visit: https://www.pwc.com/cybersecurityandprivacy
Thank you!