

Why information governance is more important than ever when it comes to protecting privacy

Legal, Compliance and Technology Executive Series



Building a better working world

Authors:

Ben Hawksworth

Managing Director, Forensic & Integrity Services
Ernst & Young LLP

Jennifer Joyce

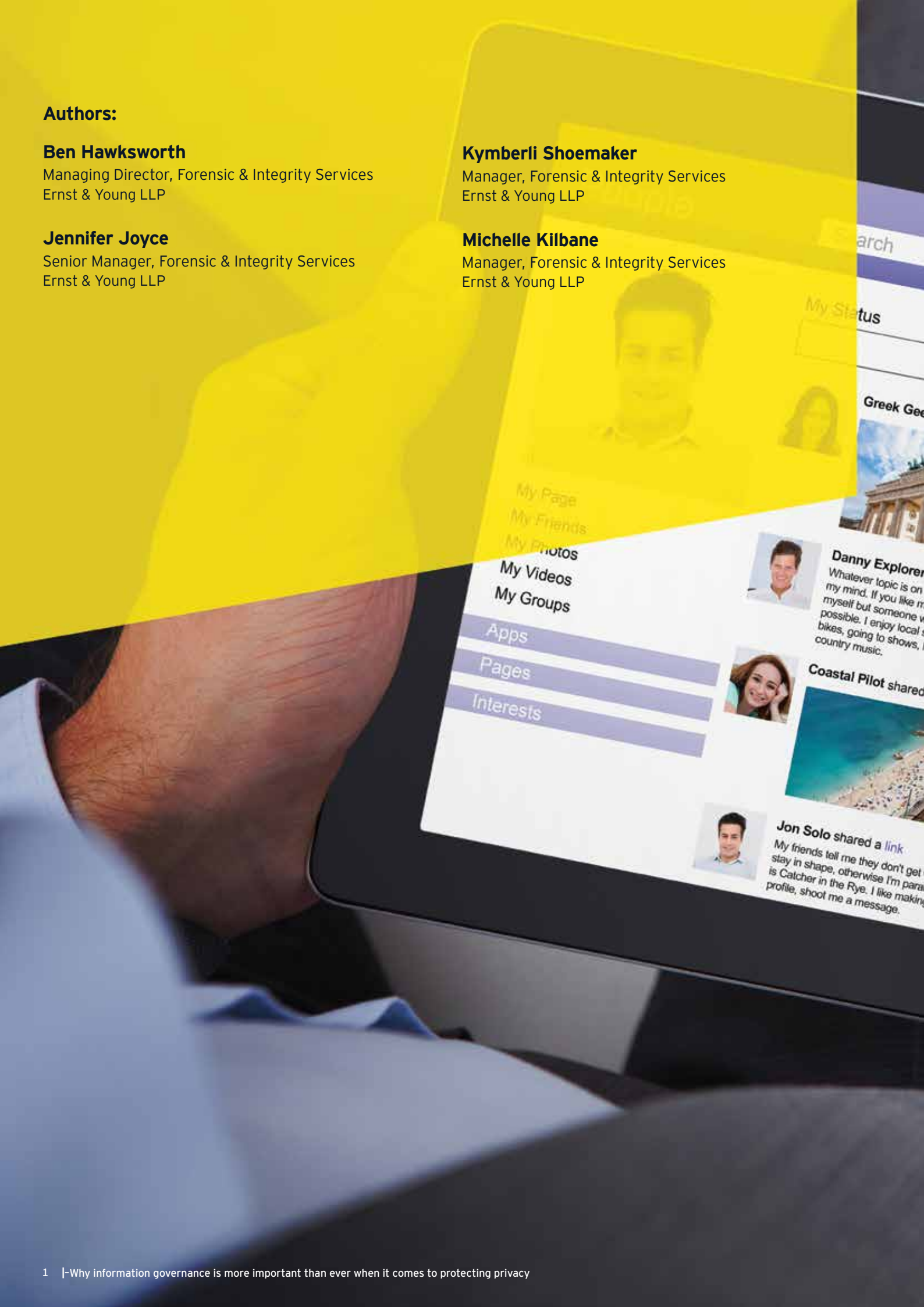
Senior Manager, Forensic & Integrity Services
Ernst & Young LLP

Kymberli Shoemaker

Manager, Forensic & Integrity Services
Ernst & Young LLP

Michelle Kilbane

Manager, Forensic & Integrity Services
Ernst & Young LLP





Introduction

2020 brought important new privacy laws in California and Brazil that left organizations scrambling. We also saw several major enforcement actions and fines for violations of the General Data Protection Regulation (GDPR), including the second-largest fine imposed to date.¹ And we faced unprecedented impacts of the COVID-19 pandemic that changed the way we as a society lived and worked, nearly overnight, bringing with it a whole host of privacy challenges that companies are still grappling with. Without a comprehensive US federal privacy law in sight, the privacy community continues to face an uphill battle with a wave of potential state data privacy laws proposed in 2021, including those introduced in New York and Virginia. By 2023, it's estimated that 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% in 2020, according to Gartner.²

But as we continue to face these evolving regulatory challenges, the essential foundation for protecting consumers' privacy remains the same – a sound information governance (IG) program. Adhering to established IG principles is essential to building a privacy program that supports an organization's legal, regulatory and business requirements, minimizes breaches and privacy incidents and establishes brand recognition for protecting consumer data.

We have developed seven principles that can serve as the foundation of an integrated IG and privacy program for any organization. In addition to reducing privacy risks, good information governance can cut costs, make processes more efficient and enable faster and more informed decision-making.



¹ 14 Biggest GDPR Fines of 2020 and 2021 (So Far): Data Protection Authority of Hamburg, Germany, fined clothing retailer H&M €35,258,707.95 – the second-largest GDPR fine ever imposed," *Tessian website*, www.tessian.com/blog/biggest-gdpr-fines-2020/, 3 February 2021."

² Hyper Cycle for Privacy, 2020," *Gartner website*, www.gartner.com, 23 July 2020.



Principle 1: Know your information

The most fundamental step for managing information and privacy risks is understanding what types of data your organization creates, receives and collects as part of its business processes. Only by understanding what data they have will organizations be able to determine the legal and

regulatory requirements with which they must comply. Privacy compliance in particular is impossible without knowing the types of personal data that are being collected and from whom.

Approaches to compliance

As a starting point, organizations should consider creating a data inventory that identifies the types of data that are most critical to the organization (e.g., intellectual property, financial documents), require special handling or protection (e.g., personal data), or are required by law or regulation (e.g., records). Inventories can then be used by companies to develop classification frameworks to identify these key data types across the enterprise.

Organizations are increasingly using advanced text analytics and various artificial intelligence (AI) technologies to inventory and classify data. Search criteria and predictive analytics are established to explicitly identify types of data and where the data is stored.

More than half of companies plan to invest in data discovery, including inventory and mapping, to improve their management of data rights, according to a 2020 IAPP-BigID survey.

Source: "The State of Data Rights," *IAPP website*, www.iapp.org, October 2020.

Principle 2: Know where you have it

Knowing what data your organization has is of little use unless you also know where it is. Organizations that can't efficiently locate personal data will be hard-pressed to demonstrate compliance with privacy regulations, including responding to data subject access requests (DSARs) within prescribed timelines, implementing proper controls for protecting personal data in systems and repositories, and implementing appropriate transfer tools and safeguards when transferring data across jurisdictions and to third parties.

Approaches to compliance

Organizations should leverage their data inventories to build a data map, which links data to systems or repositories, both within and outside the organization. Data maps are an essential tool for managing data and complying with privacy regulations, since they can be used to track data throughout its life cycle and as it moves across jurisdictions, allowing the organization to identify relevant global privacy and protection requirements.

While data discovery and mapping technology can certainly accelerate the development of a data map, a rich and comprehensive data map can be developed only with substantial engagement of the organization's business and IT stakeholders. Where technologies may prove most useful is in the ongoing maintenance of the data map, where ongoing reviews and updates to the data map can be streamlined through automation.

A data map provides the organization a holistic view of information risks, including privacy, cyber and legal discovery risks. Data maps can capture a broad range of information, including data ownership, format, consent and collection activities, business purpose and processing activities, retention and disposition practices, and access controls.



Principle 3: Know how it's being used

Given the potential risks and costs of holding on to data that has no ongoing business value, organizations should invest time into understanding the business purpose of their data. From a privacy perspective, this aids in data minimization, a principle of both the GDPR and California Privacy Rights and Enforcement Act (CPRA) requiring organizations to limit the collection, storage and use of personal data to only what is relevant and absolutely necessary for carrying out the purpose for which the data is processed.

Data minimization is equally important to an organization's IG program, as it allows organizations to focus their resources on managing and protecting their most valuable information.

Rigorous due diligence is essential to prevent third-party misuse of data and comply with regulations such as GDPR Article 28 and the California Consumer Protection Act (CCPA), both of which require organizations to use contracts to establish privacy requirements with third parties, including data life cycle management and data protection principles. The GDPR also states that data controllers are responsible for the compliance of any processor they engage.

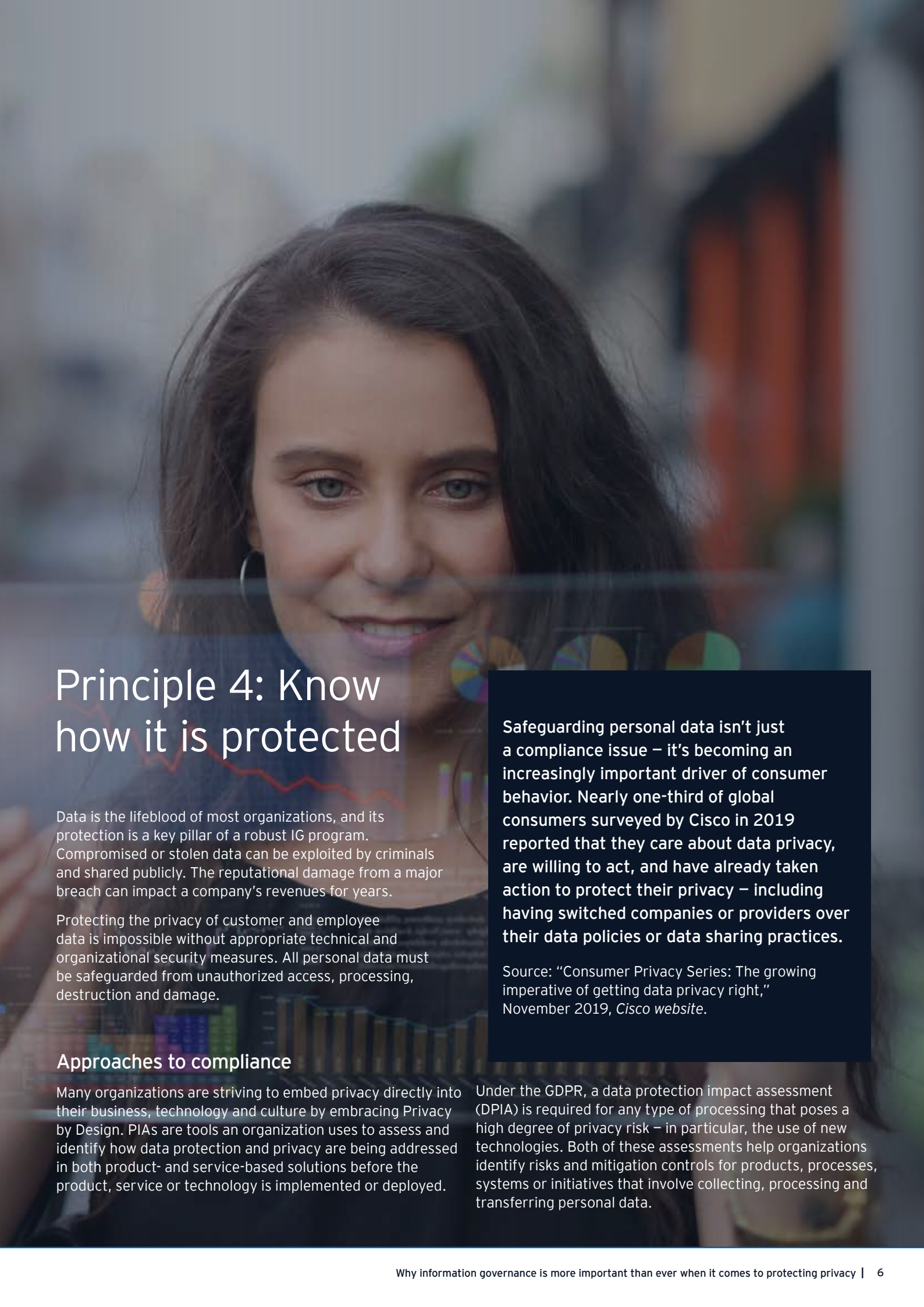
California's new privacy laws specifically give consumers the right to opt out of having their data sold or shared by the business that collected it. Organizations need to know if they are sharing or selling data and implement opt-out controls at the point of consumer data collection where necessary.

Approaches to compliance

Organizations subject to GDPR must document the purpose for which different categories of personal data are processed in Records of Processing Activities (ROPAs), as required by Article 30. This information can often be captured and updated as part of broader data mapping activities undertaken by the organization.

Organizations should consider implementing additional controls and processes to flag new processing activities, including changes to how data is being used internally or by third parties, to which data subjects may not have consented and may need to be evaluated as part of a privacy impact assessment (PIA).

Additional technology-enabled solutions, such as contract analytics, audit workflow automation technologies and other third-party risk management tools, will support privacy compliance, as well as support other business requirements and objectives related to managing third parties.



Principle 4: Know how it is protected

Data is the lifeblood of most organizations, and its protection is a key pillar of a robust IG program. Compromised or stolen data can be exploited by criminals and shared publicly. The reputational damage from a major breach can impact a company's revenues for years.

Protecting the privacy of customer and employee data is impossible without appropriate technical and organizational security measures. All personal data must be safeguarded from unauthorized access, processing, destruction and damage.

Approaches to compliance

Many organizations are striving to embed privacy directly into their business, technology and culture by embracing Privacy by Design. PIAs are tools an organization uses to assess and identify how data protection and privacy are being addressed in both product- and service-based solutions before the product, service or technology is implemented or deployed.

Safeguarding personal data isn't just a compliance issue – it's becoming an increasingly important driver of consumer behavior. Nearly one-third of global consumers surveyed by Cisco in 2019 reported that they care about data privacy, are willing to act, and have already taken action to protect their privacy – including having switched companies or providers over their data policies or data sharing practices.

Source: "Consumer Privacy Series: The growing imperative of getting data privacy right," November 2019, *Cisco website*.

Under the GDPR, a data protection impact assessment (DPIA) is required for any type of processing that poses a high degree of privacy risk – in particular, the use of new technologies. Both of these assessments help organizations identify risks and mitigation controls for products, processes, systems or initiatives that involve collecting, processing and transferring personal data.



Principle 5: Know how to respond to external events

IG principles enable a company to understand how external factors and events impact data management. Before the new breed of data privacy regulations, strong IG programs enabled organizations to respond to complex, time-sensitive, and resource-intensive requests for data stemming from

regulatory examinations, litigation and M&A transactions. Similarly, a sound IG program facilitates an organization's ability to pivot and efficiently respond to data privacy events as well, such as DSARs, privacy incidents and data breaches.

Approaches to compliance

An essential component to an IG program is to leverage knowledge from resources like data maps, and align technology to create efficiencies in identifying, collecting, reviewing and providing relevant data to the requesting party. At a minimum, standardized efficient workflows should be developed for DSAR processing.

New technologies should be considered to support compliance with privacy requirements as more people around the globe gain access rights. When considering technologies to support DSARs, for example, organizations should think holistically of the external events they may face about how existing or new tools can be leveraged to support the organization across all areas of exposure. For example, many of the tools on the market that support legal discovery may be repurposed to support search, review and redaction of unstructured data that must be provided to a data subject. The volume and frequency of these requests should be a factor considered when evaluating technology and associated costs to satisfy the external events.

DSARs have become one more external event that can put an incredible strain on organizations as they struggle to meet regulatory deadlines. More than half of organizations subject to the GDPR are missing the standard one-month deadline to respond to DSARs, according to a global Talend survey.

Source: "GDPR Compliance Rate Remains Low According to New Talend Research," 3 December 2019, *Talend website*.

Principle 6: Keep it only as long as you need

As organizations face pressure to limit their use of personal data, many are revisiting their retention policies to realign business requirements with public expectations. Just as companies work to restrict gathering personal data, they need to limit the retention of information beyond what is necessary for business purposes.

While companies historically have worked with third-party providers and law firms to develop retention schedules that identify both state and federal record-keeping requirements, along with any industry-specific requirements, many have lacked the funding, resources and internal support to keep those schedules current with the rapidly evolving privacy regulations.

Approaches to compliance

Companies should leverage privacy initiatives to draw attention to outdated retention schedules and procedures to create a more holistic approach to managing retention. Privacy-related retention limitations should be mapped so that companies have a comprehensive view of the information they need to retain, including for how long and why.

Records management systems and advanced technologies, such as AI-enhanced automation using predefined business rules, can also help organizations manage records throughout their life cycles, in accordance with relevant regulations. Systems can be configured to retain records in accordance with the schedule or defined retention requirement, while also suspending disposition in the event of a legal or regulatory matter, ultimately reducing the burden typically placed on individual employees.

The intersection of retention and privacy

The recently passed CCPA requires that companies disclose the “length of time the business intends to retain each category of personal information.” (Source: CPRA, 1798.100(a)(3))

The French data protection authority, Commission nationale de l’informatique et des libertés (CNIL), ruled that an online retailer violated storage limitation (Article 5(1)(e) of the GDPR as the retailer “did not set out any data retention policy and did not proceed to any regular erasure and achieving of clients and prospects’ personal data.” (Source: “Privacy Matters, DLA Piper’s Global Privacy and Data Protection Resource,” *DLA Piper website*) The CPRA and the GDPR requirements illustrate the importance of IG to privacy, as companies need to limit the retention of data and enforce timely disposition of that personal data, consistent with retention requirements.



Principle 7: Dispose of everything else

Disposition frameworks leverage processes and technology to remove data that no longer has value to the organization, has exceeded retention requirements, and need not be preserved under a legal hold. This allows a business to reduce privacy risks while helping control legal and business costs. Organizations must determine how to best dispose of different types of data, with some information requiring a combination of methods. A sound IG strategy is pre-emptively disposing of data before it exceeds retention requirements and propagates across systems.

Deletion requests from data subjects pose a growing privacy risk as they must be handled in compliance with relevant regulations, under strict deadlines. Under both the GDPR and CCPA, it is not enough for an organization to dispose of personal data upon request – its processors and service providers must delete that information as well.



Approaches to compliance

Technology-enabled processes allow an organization to operationalize disposition and improve efficiencies, using advanced analytics, AI and automation. The goal is routine disposition of routine, outdated and trivial information (ROT), embedded into the organizations' broader data management activities. The disposition process must be both defensible and auditable, and many organizations work with outside counsel and third-party providers to consider the legal and operational aspects of a disposition framework.

Appropriate disposition methods should be considered for each data set, which may vary based on the data and regulatory requirements associated with each data set. Disposition methods include:

- ▶ **Deletion:** permanent removal of data reduces risks and minimizes data, but makes the information unavailable for analytics or other business needs
- ▶ **De-identification:** anonymization and advanced pseudonymization techniques enable analytics while removing personal identifiability, but it may be possible to reidentify data from supporting fields
- ▶ **Aggregation:** summarizing data provides analytic insights into large data sets while removing personal information but can remove important context

In summary

As new and evolving privacy regulations make compliance more challenging, a sound IG program has become more important than ever before. An organization that reduces its data footprint can focus its resources on managing the essential information it needs for business, legal or regulatory reasons.

Organizations without effective data management policies, processes and technology will find themselves swimming in a sea of unmanaged and abandoned data that requires significant resources to maintain and clean up. This will likely require a combination of personnel and funding to remediate the issues, including an investment in privacy and data management technology and resources that can support effective adaptation to the ever-evolving privacy landscape. Technology investments and tactical moves to improve data and privacy protection are likely to prove disappointing unless an organization adheres to fundamental IG principles.

An integrated governance and privacy program requires legal and privacy professionals to partner with information security, records and data life cycle management and other functions to embed the principles described here into business processes. Organizations that do this successfully can reduce their privacy risks, control costs, increase efficiencies, improve data-driven decision-making, and foster public trust.

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

© 2021 EYGM Limited.
All Rights Reserved.

EYG no. 002782-21Gbl
WR 2102-3715486
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com