PrivacyOps

Automating Privacy Operations Across Your Organization

Rehan Jalil

PrivacyOps

Automating Privacy Operations Across Your Organization

Rehan Jalil

ISBN 978-1-7333560-0-8

www.securiti.ai

Dedication

This book is dedicated to all who are committed to making their organizations reliable custodians of sensitive personal data and comply with global privacy regulations.

This book is also dedicated to all my fellows at SECURITI.ai who are committed to making this world a safer place for online presence and sensitive personal data.

•••

Acknowledgments

This book would not have been possible without the contribution of my fellows at SECURITI.ai

In particular, I would like to sincerely thank Vivek Kokkengada, Daniel Bayat, Chaks Chigurupati, Yoshi Takebuchi and Mahrukh Rashid who enabled me to make this book a reality.
Thank you!

Contents

Notes

CHAPTER 1

PrivacyOps

The multi-disciplinary practice to grow trust-equity of your brand and comply with privacy regulations.

PrivacyOps is the combination of philosophies, practices, automation, and orchestration that increases an organization's ability to comply with a myriad of global privacy regulations reliably and quickly.

It evolves an organization from traditionally manual methods across various functional silos to full automation in a cross-functional collaborative framework for most aspects of privacy compliance. Its reliability and responsiveness to subjects enhances an organization's trust equity and makes it more trustworthy with sensitive personal data.

How PrivacyOps Works

Under the PrivacyOps model, the legal, IT, data, development, and information security teams are no longer siloed in terms of privacy compliance. Rather they operate within a common framework that lets them communicate and work more effectively toward the critical practices of privacy compliance.

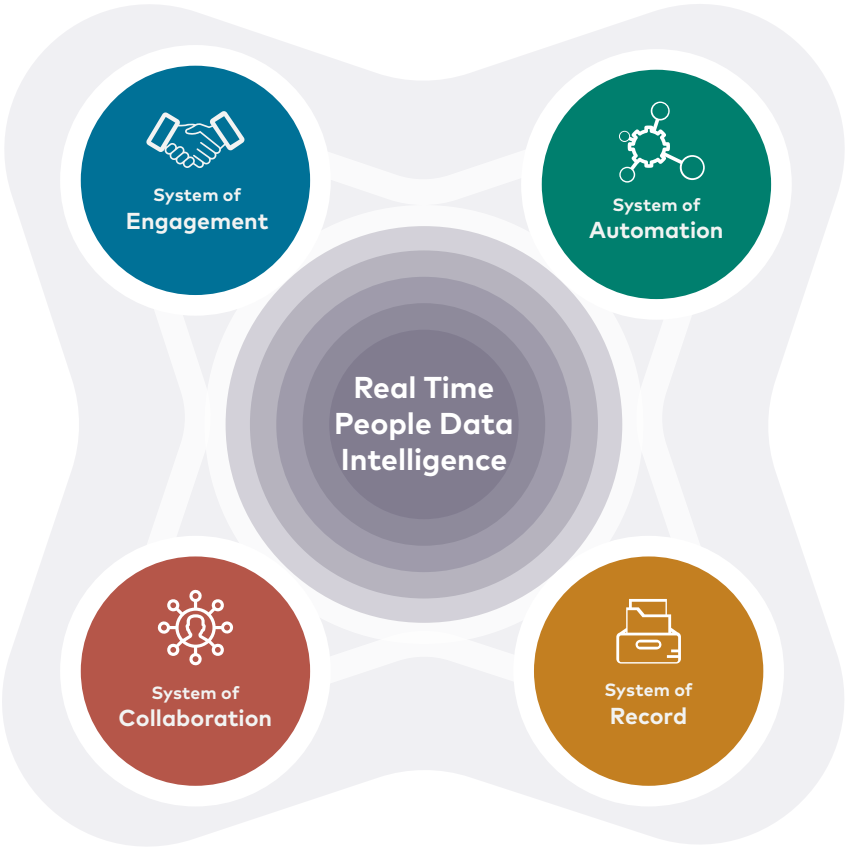
The teams use **automation** in all privacy practices that historically have been manual and slow, giving them better real-time understanding of privacy issues, readiness and compliance needs. Automation that links personal data to its rightful owner, for the purpose of user consent, makes possible the creation of People Data Graphs, which provides real-time views of regulatory risks and empowers teams to respond swiftly to compliance mandates.

PrivacyOps brings secure **collaboration** to bear on sensitive personal data. It eliminates the need for historical methods of sharing sensitive data and assessments of personal data over insecure communication channels for both compliance and review purposes. Sharing of personal data across communication channels like email and generic messaging creates further Personal Information (PI) sprawl.

Teams use **orchestration** and **robotic automation** to reliably fulfill DSRs at a much faster pace than manual methods, reducing cost and compliance risk.

Given these priorities, the general building blocks of a PrivacyOps framework must include:

- A System of Engagement & Collaboration
- A System of Automation & Orchestration
- A System of Record & Knowledge
- A System of Secure Collaboration



PrivacyOps Framework

Engage Stakeholders to Understand Privacy Posture & Risks

Automation & Workflows for Fulfilling Privacy Requirements

Securing Collaboration Among Various Stakeholders

Records, Knowledge & Analytics Informing Compliance Insight

The organizing principle of the PrivacyOps approach is that data intelligence necessarily lies at the center of all privacy compliance processes.

DSRs, Consents, Data Sharing, Breach Notifications, Internal & Vendor Assessments

Benefits of PrivacyOps

The cultural change automation, orchestration and collaboration that PrivacyOps delivers rewards you with a broad range of benefits.

BETTER UNDERSTANDING

Provide a better common understanding of data privacy regulatory obligations and compliance requirements across all functions of an organization. Teams receive a clearer view of the privacy risks lingering in personal data stored across systems, or embodied in organizational practices, related to personal data. A common PrivacyOps framework that correlates information from various privacy practices, such as readiness assessment, data discovery and linking, consent management and DSR fulfillment provides a better overall understanding of privacy posture and regulatory risks to an organization.

REAL TIME OVERSIGHT OF PRIVACY RISKS

View an up-to-date, real time display of the data privacy risks that exist inside an organization based on a) how data is collected from subjects of various residencies, b) how consent is collected along with data, c) how personal data is shared internally and externally, and d) where it is stored.

AGILITY

Move at high velocity to accomplish and maintain compliance with ever-changing privacy regulations across various geographies. Respond swiftly to DSRs from various geographies with ease, providing data subjects a satisfying and trust-building experience with your brand. Quickly notify affected subjects of any security incidents and breaches, as required by various privacy regulations. Reduce time spent on manual efforts, increasing productivity and effectiveness.

RELIABILITY

Ensure various aspects of privacy compliance across an organization, including internal assessments, vendor assessments, PI data linking, consent understanding, fulfillment of DSRs and compliance records are reliable. Increased reliability builds trust with subjects, avoids regulatory penalties, and enhances an organization's brand.

SCALABILITY

Operate various aspects of privacy practice at scale, across multiple applications, with large data sets, across different geographies and diverse stakeholders and regulations.

TIME & MONEY

To conduct business in this new, radically altered environment, we need to fundamentally rethink privacy and the methods and technologies used to secure privacy. To take just a single example—GDPR's 72-hour data breach notification window —the mandates imposed in the new Privacy Era render the "old ways" of privacy compliance completely untenable. Another example, the process of responding to DSR requests has been so resource and labor-intensive for most companies, that associated costs have been estimated to run from a rough average of $2,350 to as high as $20,000 per request.

FOCUSED EXPERTISE

Increase privacy understanding and expertise of diverse teams across an organization by having them spend more time on expert-level tasks rather than manual and mundane tasks related to assessments, DSR fulfillment, data discovery and subject communication.

IMPROVED BRAND

Develop a unique market position through trust-based relationships with both prospective and current clients. Providing transparency on data handling practices and quickly fulfilling access requests builds trust. The prospect of implementing a secure and transparent PrivacyOps infrastructure nurtures further awareness of the emerging need to adopt such practices on an industry-wide scale. This coincidentally serves as a motive for developing standardized PrivacyOps practices and therefore, a possible market niche for a singular platform.

SECURED COLLABORATION

Enable effective collaboration across diverse teams, from legal, privacy, IT, cybersecurity, marketing, development and corresponding support groups. Enable collaboration around sensitive PI data, without the need to share sensitive PI data over generic email and messaging tools.

Why PrivacyOps Matters

The use of software and data is revolutionizing the world and all aspects of life. Increasingly, organizations use personal data to craft individualized brand experiences for consumers. As a result, these organizations must store and manage more and more personal data of various kinds, including identity, activity, financial, medical and genetic. This implicit or explicit sharing of personal data by subjects sits on a delicate fabric of trust that, if compromised, causes serious harm to an organization's brand, as well as opening it to regulatory fines and lawsuits.

To understand why PrivacyOps matters, we must first understand prevailing attitudes towards personal privacy among consumers around the world. The emergence of California's Consumer Privacy Act (CCPA) and the EU's General Data Protec-

tion Regulations (GDPR) and similar laws in Brazil, Australia and other countries reflect a groundswell of sentiment that an individual's right to privacy vs. business organizations' right to collect, process and otherwise leverage personal data for commercial gain had gotten out of balance. With these privacy laws continuing to come into effect, the business environment also continues to evolve, specifically along lines where incentives to protect customer data have become imperatives. Privacy is now business critical.

Clearly, privacy compliance must now be automated across the multiple processes involved in the overall operation. The key technological capabilities powering the PrivacyOps approach must include:

- **Automated Data Searching & Linking within on-premises and cloud environments to quickly uncover personal information within multi-gigabyte data stores.**
- **Relationship Mapping between data and its owners makes it possible to compile comprehensive People Data Graphs for individual customers in operational timeframes—minutes, not days.**
- **AI-powered Data Intelligence to orchestrate review processes, and automatically assign follow-on tasks to individual data source owners and privacy team members.**
- **A Secure Workspace that enables stakeholders to collaborate on review and legal approvals while also a) preventing sprawl into non-secure channels and b) consistently logging all tasks to meet compliance reporting needs.**

With PrivacyOps, multiple teams collaborate and make full use of automation and orchestration to understand privacy posture, eliminate privacy risks and swiftly fulfill privacy obligations. This methodology engenders trust and instills confidence in an organization.

How to Adopt a PrivacyOps Model

Adopting PrivacyOps requires a cultural mindset of collaboration across traditionally siloed teams to achieve privacy compliance. PrivacyOps helps remove the silos separating various teams, such as legal, compliance, IT, cybersecurity, marketing and development. It enables each stakeholder to complement their expertise with that of every other team member. Maximum use of automation and orchestration brings efficiency, reliability and velocity in maintaining compliance with multiple privacy regulations and honoring data subjects' rights to exercise control over their personal data.

Following are the Critical Elements Required for Adopting a PrivacyOps Model

PEOPLE DATA GRAPHS—BEYOND MANUAL PI DATA LINKING

PI data linking is the process of discovering personal information stored across all systems and linking it to the owner of that personal data. With the large amount of structured and unstructured data across a vast variety of systems in an organization, this aspect must be automated. With the mandates imposed by CCPA and GDPR, static data flow maps collected from stakeholders are no longer sufficient and must be supplemented with automated data flow mapping.

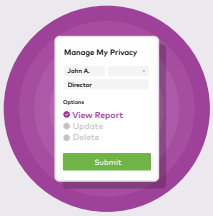
Today's regulatory environment demands the ability to create and use People Data Graphs. Far more advanced than manual data maps, People Data Graphs provide unprecedented insight into compliance risk factors. They precisely locate and identify data within your organization's IT infrastructure to show relationships between individuals and any number of PI attributes. The People Data Graph is a direct manifestation of the PrivacyOps approach, placing data at the center of all compliance processes and operations.

With the PrivacyOps approach, some data can be linked ahead of time and some can be linked on demand at the time of compiling a People Data Graph (PDG). This flexibility is indispensable in supporting compliance processes, such as managing consents and fulfilling DSRs. automatic PI data linking must be enabled across all systems, including internal, third-party, Software as a Service (SaaS), and Infrastructure as a Service (IaaS) systems. In either case, applying automation to create this link between the PI data and its owner becomes the foundation for carrying out the full range of privacy compliance tasks.

DSR FULFILLMENT AUTOMATION

DSR fulfillment is the process of receiving data requests from subjects and taking the necessary steps across all the organization's internal and third-party systems to comply with the subject's legal request. As the subject's personal data may be spread across any number of data systems managed by different stakeholders, manual methods for fulfilling the requests are highly inefficient, costly and prone to error. Moreover, when the volume of subject requests increases due to internal or external events, manual approaches to fulfilling DSR obligations bring operational hazards and compliance risks.

DSR fulfillment automation is not simply about capturing subject requests, and assigning them to different stakeholders based on some set of static rules. It is the process of fully automated discovery of systems and objects carrying subjects' personal data, and assisting system and object owners by orchestrating the DSR fulfillment review process. This is most effectively done by automatically assigning follow-on tasks to individual data source owners and privacy team members who can then collaborate on reviews and legal approvals in a secure workspace before ultimately providing the completed reports back to the subject.



SECURE PRIVACY PORTAL

As privacy regulations give data subjects rights to the personal data that organizations collect either directly or indirectly, organizations must have a secure way to collect subject requests, verify the identity of the subject, provide personal data securely to the subject all while keeping compliance records to inform audits or defend against any legal suits. Providing a secure privacy portal to subjects helps build trust, promotes a satisfying user experience, and facilitates automation for user identity verification and DSR fulfillment.

USER CONSENT LIFECYCLE MANAGEMENT

Most privacy regulations prohibit the processing of personal data unless an organization can establish legitimate interests, or the data subject has consented to the processing. Furthermore, regulations also specify that consent must be freely given, informed and unambiguous. Depending on the scenario, consent collection may be explicit (opt-in) or optional (opt-out) and if an organization chooses to rely on consent for any part of the processing, it must also be prepared to respect that choice and stop that part of the processing if the individual later withdraws consent. In other words, if an organization wants to process data lawfully and relies on consent as the lawful basis for that processing, they must implement a robust consent management system.

To establish a lawful basis for processing personal data through consent, organizations must have methods to display unambiguous notification messages at every consent collection point. Once collected, consent should be linked to unique identities and personal data records within the environment and tracked through its lifecycle so that appropriate remediation steps can be taken when the data subject withdraws consent.

BREACH NOTIFICATION AUTOMATION

Many privacy regulations require that when a case of a data breach or theft of sensitive personal information from an organization occurs, all impacted subjects must be notified in a short amount of time. As noted above, the EU General Data Protection Regulations (GDPR) require breach notifications be delivered within 72 hours. To comply with such a short timeline for notifying impacted subjects, organizations must have methods to locate PI data stored in a variety of systems, link PI data to its rightful owners, and have a playbook to automatically execute a shortlist of impacted subjects, and notify them through secure methods.

In years past, organizations would commonly err on the side of caution, and send out notifications to anyone and everyone whose data may have been compromised - even in the absence of solid evidence that the PI of the entire customer base had been exposed. With the stricter reporting mandates under CCPA and GDPR, that shotgun approach is no longer tenable as it exposes the organization to unnecessary and intolerable legal and financial risk.

The PrivacyOps approach with automated People Data Graph technology enables organizations to tightly define the pool of customers (or subjects) whose PI has been compromised. With the ability to quickly narrow the scope of who is impacted in case of data breach incidents, it becomes possible to limit which customers need to be notified, and deliver those notifications within tight reporting windows. In this way, accurately defining the pool of customers whose PI has been compromised can establish a baseline for financial liability, and provide some predictability at a very uncertain time.

PRIVACY ASSESSMENT AUTOMATION

Privacy regulations require that all internal systems carrying personal information go through an assessment process to reveal any gaps against the regulations and put controls in place to fill them and comply with regulations. These assessments must be updated on a regular basis. Multiple stakeholders typically must be involved in understanding gaps and tracking new controls to be put in place.

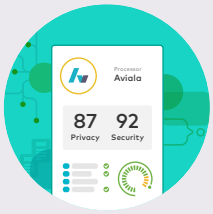
Performing these assessments over spreadsheets and emails is tedious, time consuming, prone to error, and raises difficulties in tracking the great number of systems and processes involved. Sharing selective assessments with third parties manually over emails is inefficient.

Adopting a ***system-of-knowledge*** that provides audit templates for various privacy regulations, a ***system-of-record*** to keep all assessments in one place, a ***system-of-engagement***—to bring all stakeholders together so they may provide their input—and a ***system-of-sharing*** to share assessments with external parties, makes the assessment process agile, easier to track, and up to date.

VENDOR ASSESSMENT AUTOMATION

Privacy regulations require that all third parties with whom personal information is shared go through an assessment process to understand their gaps against the regulation. These assessments must be updated on a regular basis. Performing these assessments with a large number of vendors over spreadsheets and email is tedious, time consuming, prone to error and is hard to track.

Adopting a ***system-of-knowledge*** that provides audit templates for various privacy regulations, a ***system-of-engagement*** to invite all vendors in one place to complete their assessment and a ***system-of-record*** to keep all vendor assessments and proof compliance in one place makes the vendor assessment process agile, easier to track and up to date.



VENDOR PRIVACY RISK MONITORING

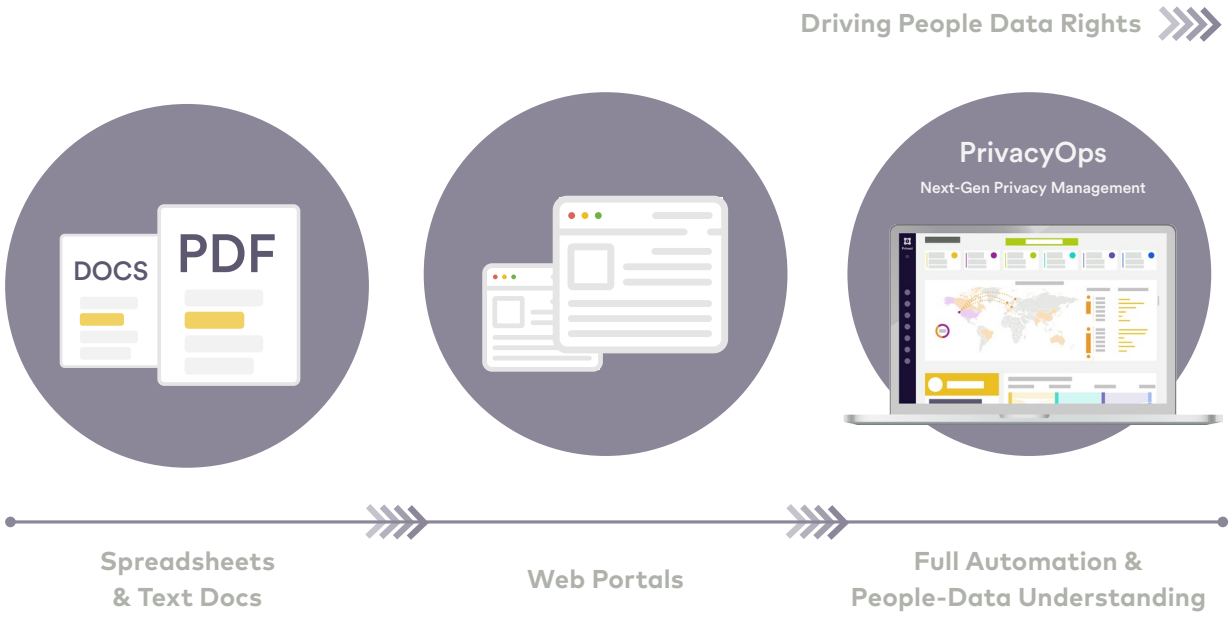
As vendors hold important personal information, it's important to monitor and rate vendors based on how they collect, store and exchange personal information with others, how they respond to DSRs, and whether they have had any recent data breaches. These independent privacy ratings of vendors supplement the responses vendors provide as part of vendor assessments audits.

Having a process in place to monitor any decline in independent privacy ratings of a vendor that falls below a certain threshold enables an organization to deal with privacy issues swiftly and responsibly.

The Evolution of Privacy Compliance

Compliance solutions have evolved from manual surveys that capture a snapshot in time coupled with simple workflow management. While the advent of web portals has improved the user experience, these solutions still lack the true end-to-end automation needed for agile and accurate privacy compliance.

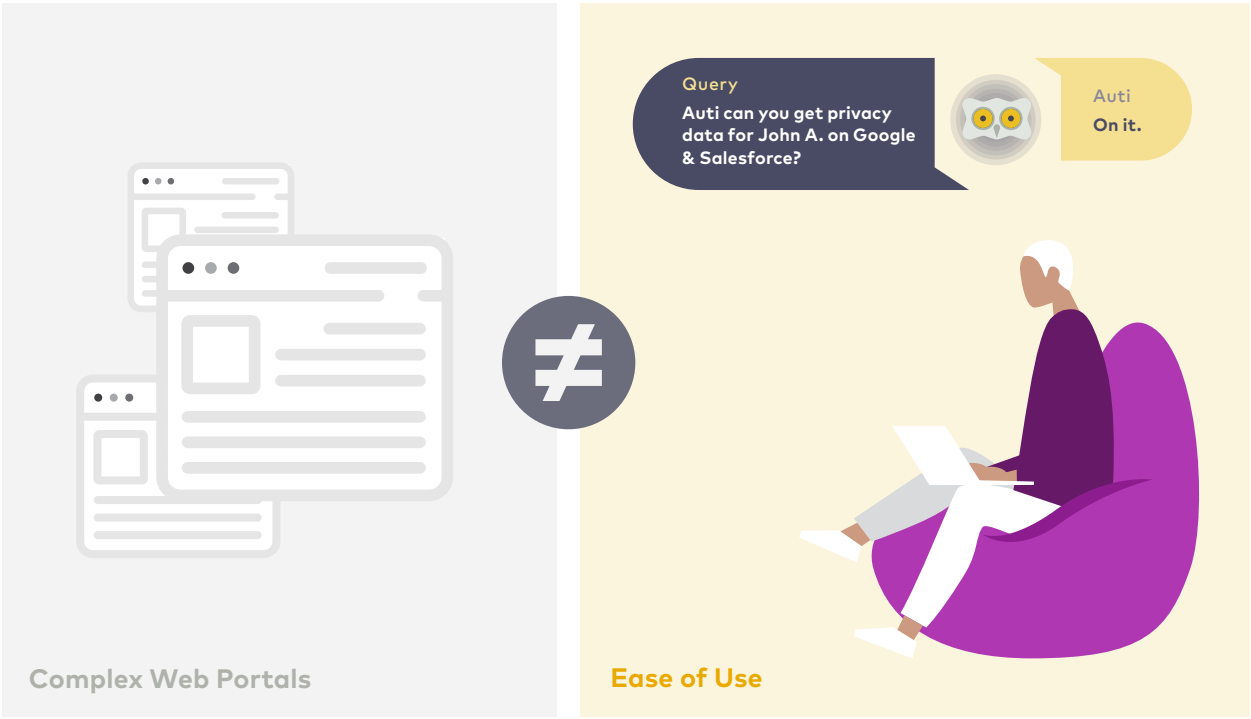
Market Evolution



Manual Workflows ≠ Automation

Many GRC or legacy compliance solutions assist with managing workflows throughout an organization to support compliance. However these solutions do not provide true automation, as they still rely on manual surveys or other inputs to the system, and they do not automate the detailed tasks and subtasks required for fulfilling privacy compliance requirements.

Web Portals ≠ Ease of Use



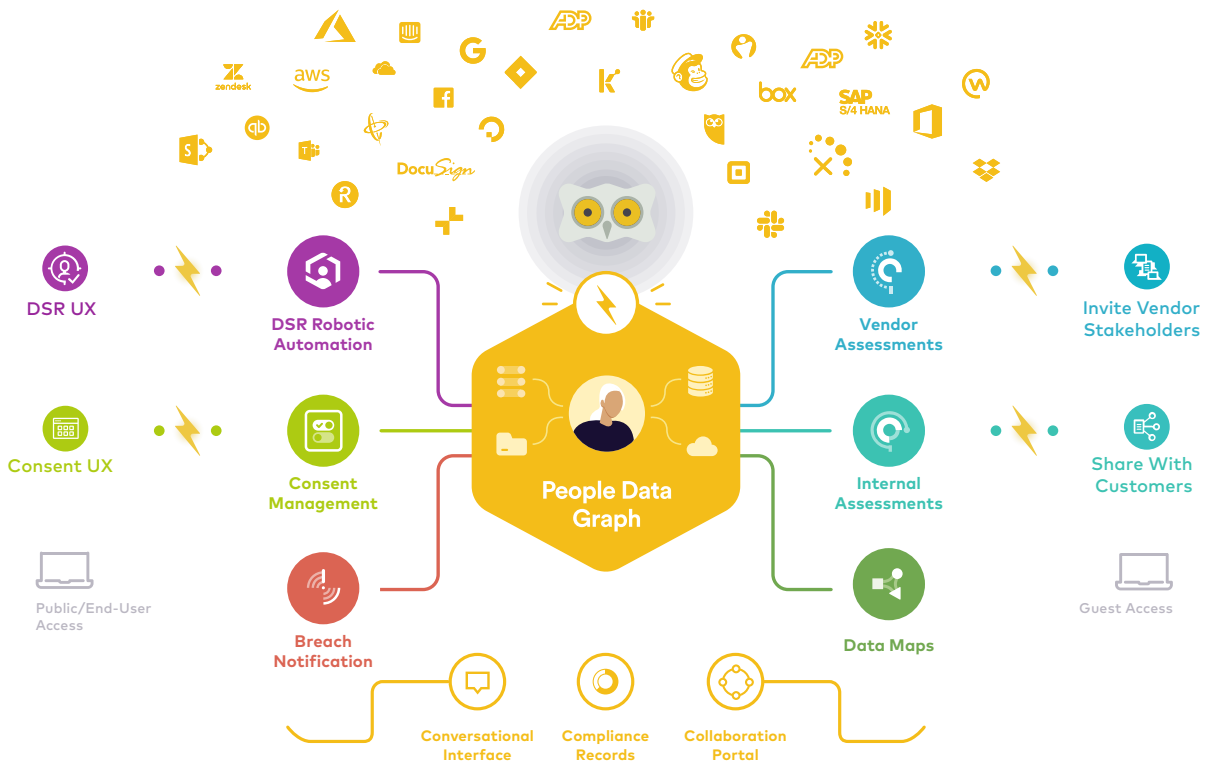
Privacy compliance is often the responsibility of legal risk and compliance professionals, that have no patience for complex technology. While web portals are an improvement over manual spreadsheets, modern privacy compliance solutions need to be easier to use, including features such as natural language interface to readily find information from complex systems.

Collaboration

Complying with privacy regulations requires collaboration across multiple functions, including legal, IT, cybersecurity, marketing, product development, etc. To avoid the sprawl of PI data, collaboration must be brought into a PrivacyOps framework, versus sending personal information to other stakeholders over unsecure email and generic messaging tools. PrivacyOps requires a built-in system of secure collaboration that minimizes data sprawl caused by distribution of sensitive personal data for reviews and approvals.

Automation & Orchestration

Automation and orchestration are at the epicenter of enabling agility, reliability, scalability and manageability for PrivacyOps. They also enable functional teams to focus on higher-level issues of privacy compliance, versus spending time and effort on mundane manual tasks.



CHAPTER 2

People Data Graph Automation

Most enterprises have hundreds or even thousands of internal and external systems in which personal data of consumers is stored, in structured and unstructured forms.

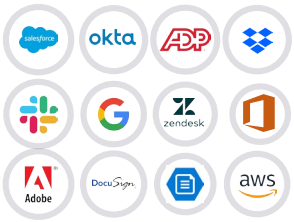
These systems include internally developed applications, internal storage systems, third-party applications, SaaS, IaaS and even end-point devices. These systems are owned by different groups and functions. Personal data in these systems can change at any moment. Data can easily sprawl between systems and even across third parties, with little traceability. Not knowing whose data is where, in real-time, across an organization, makes it extremely challenging to comply with privacy regulations and build trust with consumers.

Data can easily sprawl between systems & even across third parties, with little traceability.

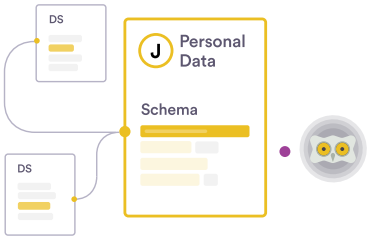
To comply with privacy regulations and smoothly fulfill a DSR or quickly comply with subject consent changes, it is not sufficient to simply apply standard data classifications to understand where PI data exists within organizations. Those organizations must also implement automatic linking of personal data to its owner.

Automation is essential for PrivacyOps to identify personal data and then link it to the data owner in order to create comprehensive, accurate People Data Graphs. Artificial intelligence plays a crucial role in the auto-discovery process of personal data and in establishing a relationship between that data and its owner. Robotic assistance is essential to automatically scan all data sources periodically, and to generate—on demand—individual People Data Graphs that are ready to access and use.

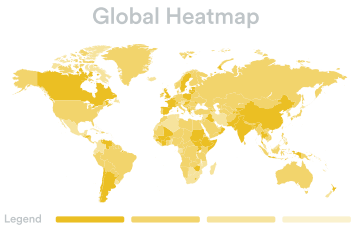
People Data Graph Automation



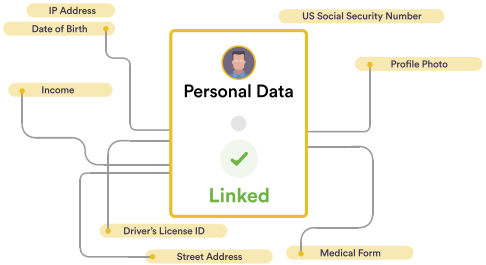
Connect AI-powered bot to your data systems



Intelligent data scanning



Build PI heatmap across systems and geographies



Automatic discovery and linking of personal data to user

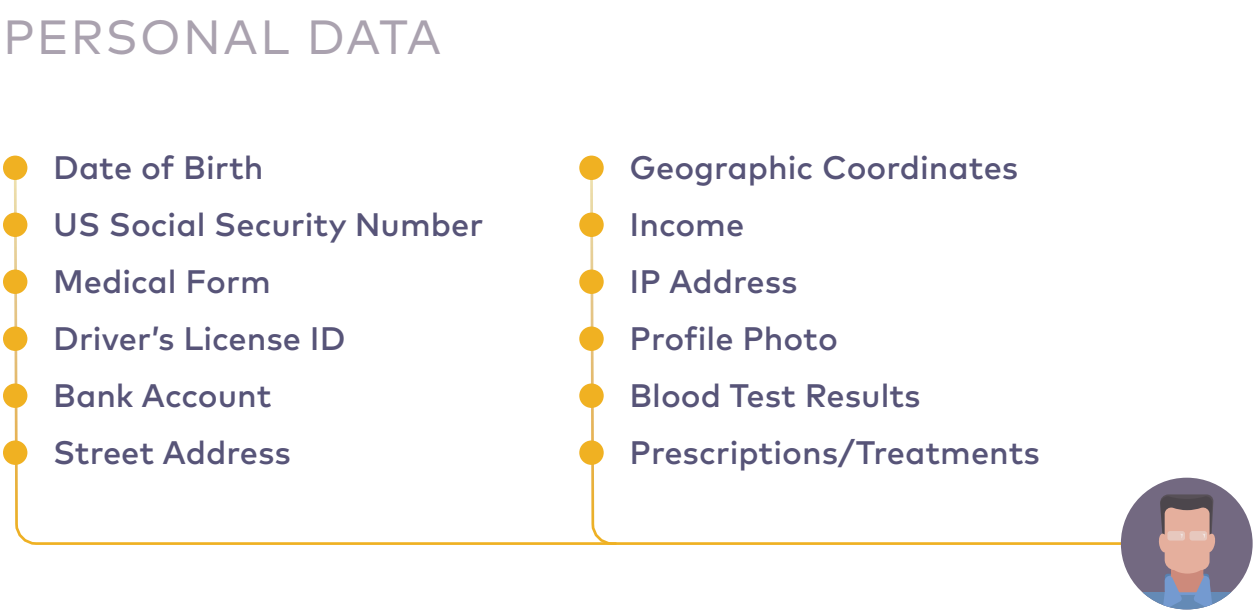
Ask AI-powered bot about personal data across systems

Submit complex data requests

Get insights about personal data from AI-powered bot

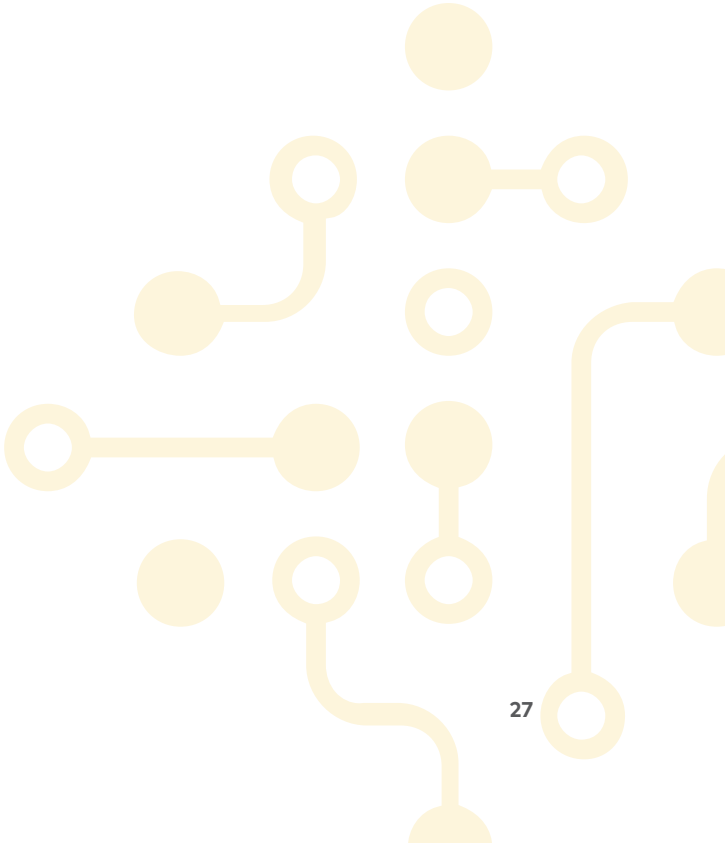
The PrivacyOps approach puts personal data intelligence at the center of all privacy compliance processes. It brings to bear the power of automated mapping to create People Data Graphs that provide the foundation for:

- Automated DSR fulfillment
- Mapping the regulations that apply to certain personal data
- Assessing data compliance risks, such as violations related to data location and residency of data owner
- Compliance with personal data retention policies
- Generating accurate internal assessments and vendor risk profiles.
- Quickly managing subjects' changes to consent profiles
- Obtaining comprehensive views of the scope of data breach or theft incidents to support tightly focused notification programs

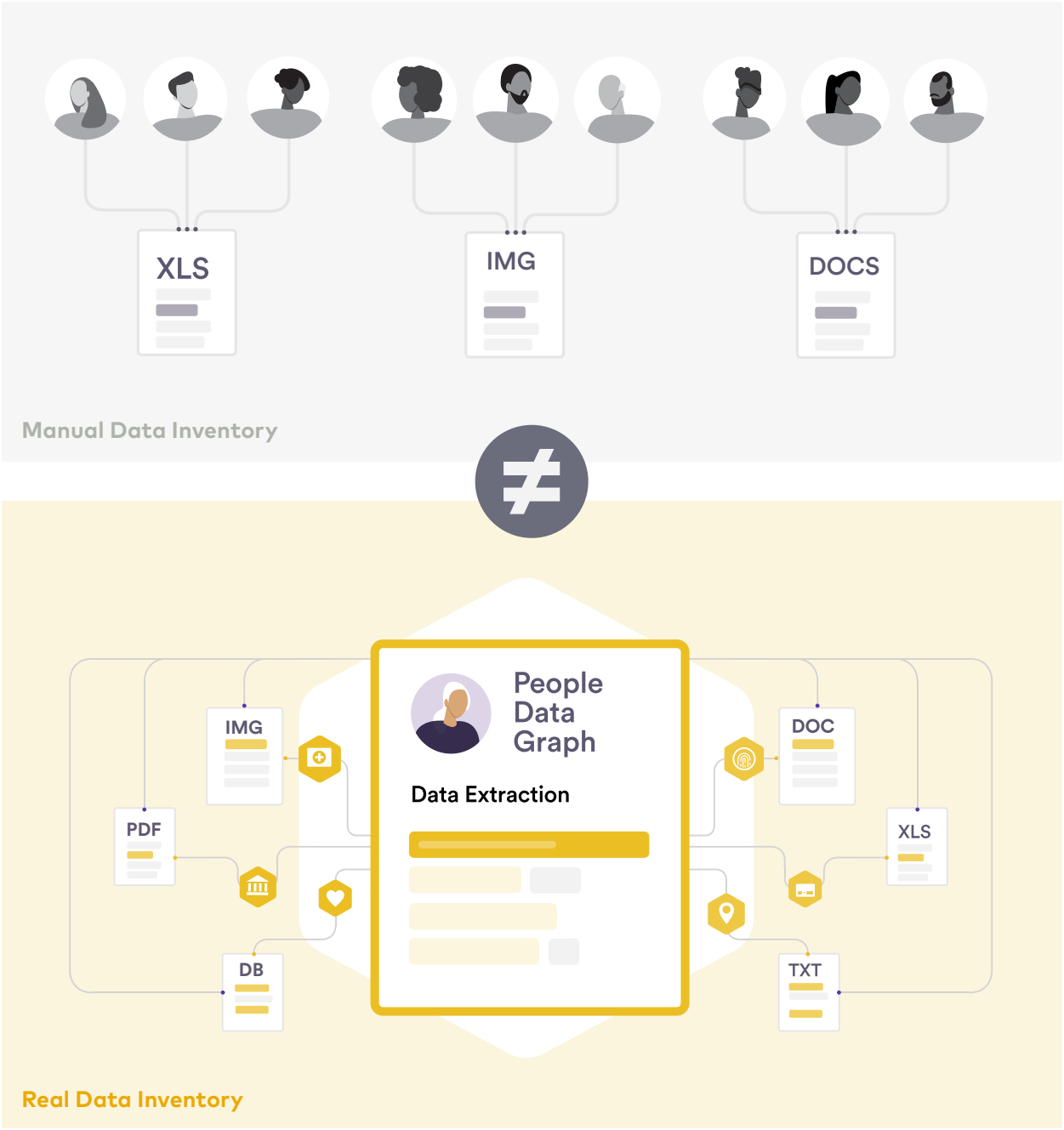


The Evolution of Data Discovery

Traditional methods of manual data mapping, data classification and eDiscovery were not designed to accommodate modern privacy regulations. While these solutions work fine for their intended use cases, regulations such as CCPA, GDPR, LGPD and others require real-time granular knowledge of personal data and its associated owner across a sprawling IT ecosystem. Automating the creation of People Data Graphs is critical for meeting these requirements and building a PrivacyOps framework.

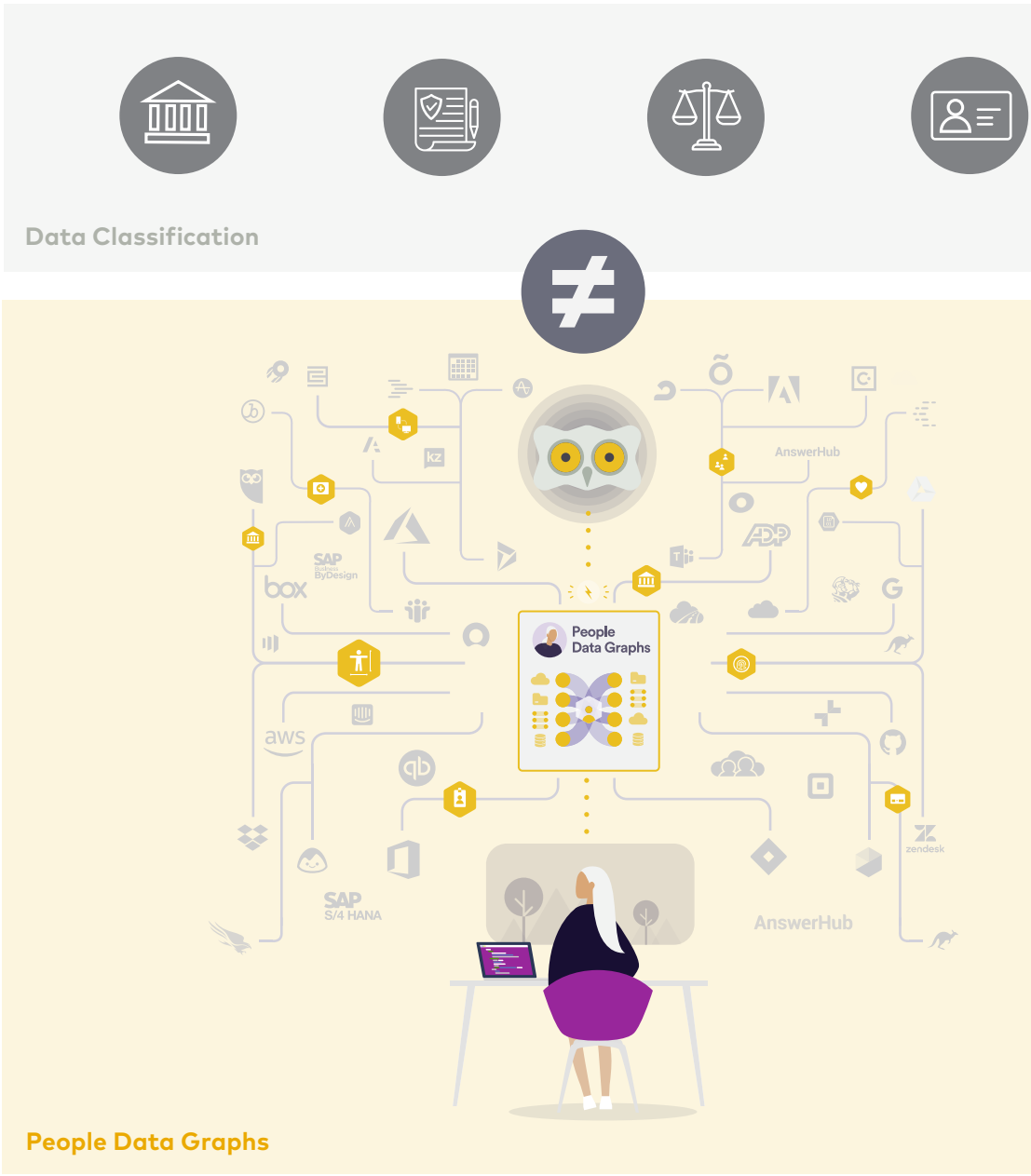


Manual Data Inventory ≠ Real Data Inventory



Manual data mapping is cumbersome, and does not scale to meet the current environment where data is highly dynamic and privacy regulations require rapid and accurate identification of personal data.

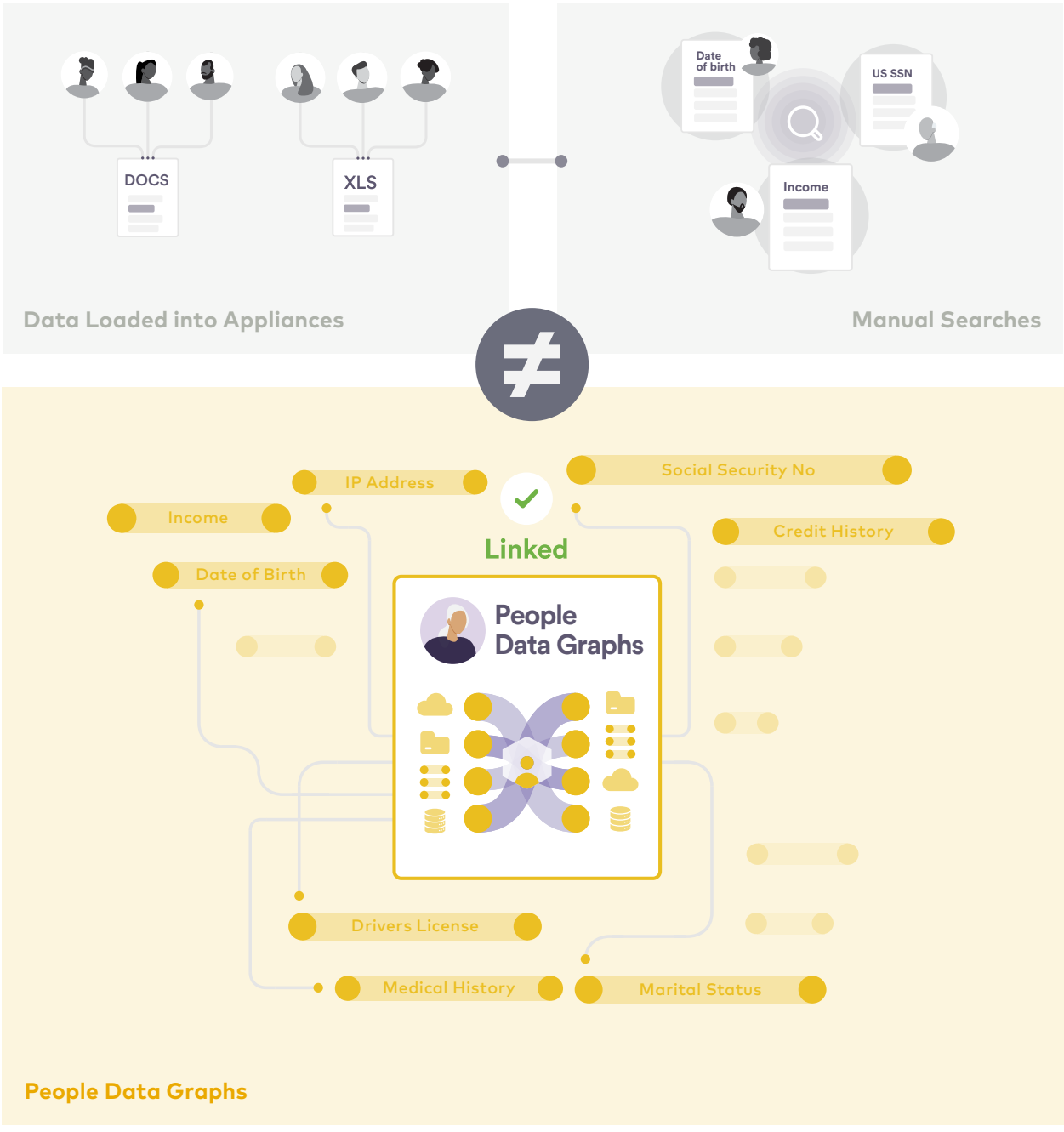
Data Classification & Discovery ≠ People Data Graphs



People Data Graphs

Data classification and discovery technologies, such as DLP, classify data in categories (e.g., PII, confidential, sensitive). However, these systems have no understanding of an individual's information, nor do they provide any automation to manage an individual's data for privacy purposes.

eDiscovery ≠ People Data Graphs



eDiscovery solutions aid with legal discovery, but they require data be loaded into an appliance or system. This can exasperate PD sprawl, and has challenges scaling to the vast number of data stores that may hold personal data.

Why Automation is Essential

PrivacyOps is rooted in the real-time understanding of personal data within your organization. This is fundamental to enabling an agile, efficient compliance program that can address the new privacy landscape.

The implementation of GDPR, CCPA and other privacy regulations reflect a major change in attitude toward personal privacy. This new public consciousness, that one's personal information must be rigorously protected by organizations that collect it, is reshaping how organizations view privacy compliance. In a commercial environment where the customer is empowered to assert their rights over their personal information, companies that are most attentive and responsive to those rights will stand out as privacy champions.

Given these realities, the ability to locate and map personal information to specific individual identities to create People Data Graphs is now a privacy compliance imperative. Indeed, the vivid, accurate, richly detailed views of your customers and their data contained within People Data Graphs will resonate through all aspects of your privacy compliance program, empowering you to thrive in the new Privacy Era.

WHAT IS PERSONAL DATA (PD)?

"Personal information" or "Personal Data" includes the following information when it identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular data subject or household.

IDENTIFIERS

Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

"Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer or family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

For purposes of this definition, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

RECORDS

Any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. (All PI also fits into this category by definition).

CHARACTERISTICS OF PROTECTED CLASSIFICATIONS

Subject to legal determinations, but could include: race, color, ancestry, national origin, citizenship status, religion, sex (including pregnancy, childbirth, and related medical conditions; including titles such as Mr./Mrs.), disability (Physical or mental), age (40 and older, but any age collection would be PI), genetic information, marital status (including titles such as Mrs.), sexual orientation, gender identity and gender expression, AIDS/HIV status, medical condition, political activities or affiliations, military or veteran status, and status as a victim of domestic violence, assault, or stalking.

COMMERCIAL INFORMATION

Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

BIOMETRIC INFORMATION

An individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY INFORMATION

Including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet web site, application, or advertisement.

GEOLOCATION DATA

Not clearly defined, but likely includes programmatically generated (as opposed to manually entered) information that can be used to identify an electronic device's physical location at some point in time.

AUDIO, ELECTRONIC, VISUAL, THERMAL, OLFACTORY, OR SIMILAR INFORMATION

Not clearly defined, but likely includes information generated from Internet of Things (IoT) devices: smart speakers, home security devices and information such as a person's olfactory fingerprint.

PROFESSIONAL OR EMPLOYMENT-RELATED INFORMATION

Includes any information indicating professional or employment status, collected in the context of professional activity or employment, or relating to professional or employment activity, qualification, performance, etc.

EDUCATION INFORMATION

Non-public information directly related to a student and maintained by an educational agency or institution or by a person acting for such agency or institution. Some exceptions may apply.

INFERENCES

Inferences drawn from any of the information identified in this section to create a profile about a consumer reflecting their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

ANY OTHER PI

Any information other than that specifically categorized above that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

This definition means any information that "is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is personal information, unless one of the exceptions in the state applies. For example, business contact information, device ID numbers, even the location of a warehouse (for example, if it's in a field identifying it as the closest warehouse to a consumer's delivery address) can all be personal information.[1]

The provisions of most regulations are not limited to information collected electronically or over the internet, but apply to the collection and sale of all personal information collected by a business from consumers.

"Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.

"Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.[2]

1 Cal. Civ. Code § 1798.175

2 Cal. Civ. Code § 1798.140 (o)(2)WW

Categories of Personal Data

INTERNAL

Authentication

Authentication information belonging to the person

PASSWORDS, MOTHER'S MAIDEN NAME, ETC.

Knowledge & Belief

What a person knows or believes

THOUGHTS, RELIGIOUS BELIEFS, ETC.

Preference

A person's preferences or interests

LIKES & DISLIKES, INTENTIONS, OPINIONS, ETC.

EXTERNAL

Behavioral

A person's online/offline behavior

BROWSING HISTORY, CALL LOGS, ATTITUDE, ETC.

Demographic

A person's characteristics

AGE, INCOME, GEOGRAPHIC, PHYSICAL TRAITS, ETC.

Ethnicity

A person's ethnic origins

RACE, LANGUAGE, DIALECTS, ACCENTS, ETC.

Identifying

Unique information that identifies a person

NAME, GOVERNMENT-ISSUED ID, BIOMETRIC DATA, ETC.

Categories of Personal Data, Cont'd

Medical & Health

Health status & medical conditions of a person

OVERALL HEALTH, TEST RESULTS, FAMILY HEALTHHISTORY, ETC.

Physical Characteristics

A person's physical traits

HEIGHT, SKIN COLOR, EYE COLOR, ETC.

Sexual

A person's sexual life & preferences

GENDER IDENTITY, PREFERENCES, ETC.

FINANCIAL

Account(s)

A person's financial account(s)

BANK ACCOUNT NUMBER, CREDIT CARDNUMBER, ETC.

Credit

A person's financial credit & reputation

CREDIT RECORDS, CREDIT CAPACITY, ETC.

Ownership

Items a person owns/rents/etc.

HOUSES, CARS, BOATS, ETC..

Transactional

Income & spending of a person

PURCHASES, SALES, LOANS, ETC.

Categories of Personal Data, Cont'd

SOCIAL

Communication

Any communication a person is involved

RECORDINGS OF PHONE CALLS, EMAIL, ETC.

Criminal

A person's criminal activity

CHARGES, CONVICTIONS, ETC.

Family

A person's family & relationships

FAMILY STRUCTURE, MARRIAGE HISTORY,RELATIONSHIPS, ETC.

Professional

Educational or professional career

EMPLOYMENT, SALARY, CERTIFICATIONS, ETC.

Public

A person's characteristics

AGE, INCOME, GEOGRAPHIC, PHYSICAL TRAITS, ETC.

Ethnicity

A person's public life

GENERAL REPUTATION, MARITAL STATUS, POLITICAL AFFILIATIONS, ETC.

Social Network

Friends or social connections

FRIENDS, CONNECTIONS, ASSOCIATIONS, ETC.

Categories of Personal Data, Cont'd

HISTORICAL

Life Events

History of events that might haveinfluenced a person's life

WARS, RIOTS, ETC.

TRACKING

Contact

Ways to contact a person

EMAIL ADDRESS, PHONE NUMBER, ETC.

Device

Devices that a person uses

IP ADDRESS, MAC ADDRESS, ETC.

Location

A person's physical location

COUNTRY, GPS COORDINATES, ETC...

CHAPTER 3

Data Subject Rights Fulfillment Automation

Modern privacy regulations such as CCPA and GDPR grant consumers broad rights to the personal data that enterprises collect from them and about them.

Depending upon their location, consumers can request access to their data, request that an organization stop processing it, or request it be deleted. Enterprises must fulfill such requests promptly, with only a few exceptions allowed for legal reasons. Each request from a consumer can translate into large numbers of often ill-defined tasks that you must perform inside your company.

Without an automated system to correlate identity and personal data, the resolution of such requests can translate into manual investigations in order to:

- Verify the identity of the person making the DSR.
- Discover which systems and which objects within those systems hold the subject's data. A typical enterprise may have hundreds or thousands of such internal and external systems.
- Discover current owners of those systems and objects. In a typical enterprise, the ownership changes regularly.
- Engage owners of systems and objects over email or other methods and share the details of the subject.
- Work with each system and object owner to comply with the request. The actions required vary depending upon the request type and the legal reasons for data retention.

- **Combine the products of all parts of the investigation into one report for approval by the stakeholders and the legal team.**
- **Securely share the report with the data subject.**
- **Keep an audit trail of all the steps taken to comply with the request and prove compliance in case of legal issues.**

Doing all of the above tasks manually for each subject request is costly, inefficient, and most importantly, prone to human error and lapses of compliance.

Manual fulfillment of DSRs is laborious, inefficient, and prone to costly errors.

PrivacyOps assisted by AI and bots helps automate and orchestrate most of the manual tasks listed above to swiftly fulfill DSRs, and enables secure collaboration between stakeholders for review and approvals.

AI & bot assisted PrivacyOps:

- **Automatically discovers systems and objects that hold subjects' data, across hundreds or thousands of internal and external systems. It identifies current owners of those systems and objects.**
- **Automatically invites all owners and stakeholders to collaborate securely in one platform, centered around tasks and subtasks.**
- **Automatically collects or assists in collecting the subject's personal data from each system and makes it available for review and approval.**

- Automatically enables collaboration, review, and approvals around the subject's personal data in one platform, rather than spreading personal data further in emails and other messaging systems for reviews and approvals.
- Automatically generates a report for the subject.
- Automatically keeps an audit trail of all the steps taken to comply with the subject request, to prove compliance in the event of legal issues.

With automated PrivacyOps, you can let AI & bots help fulfill the DSR requests for you.

Secure Privacy Portal for Customer Communications

As privacy regulations give rights to consumers over their personal data that enterprises collect directly or indirectly, they are entitled to request access, processing stoppage, or deletion of their data.

Following are many aspects that must be resolved:

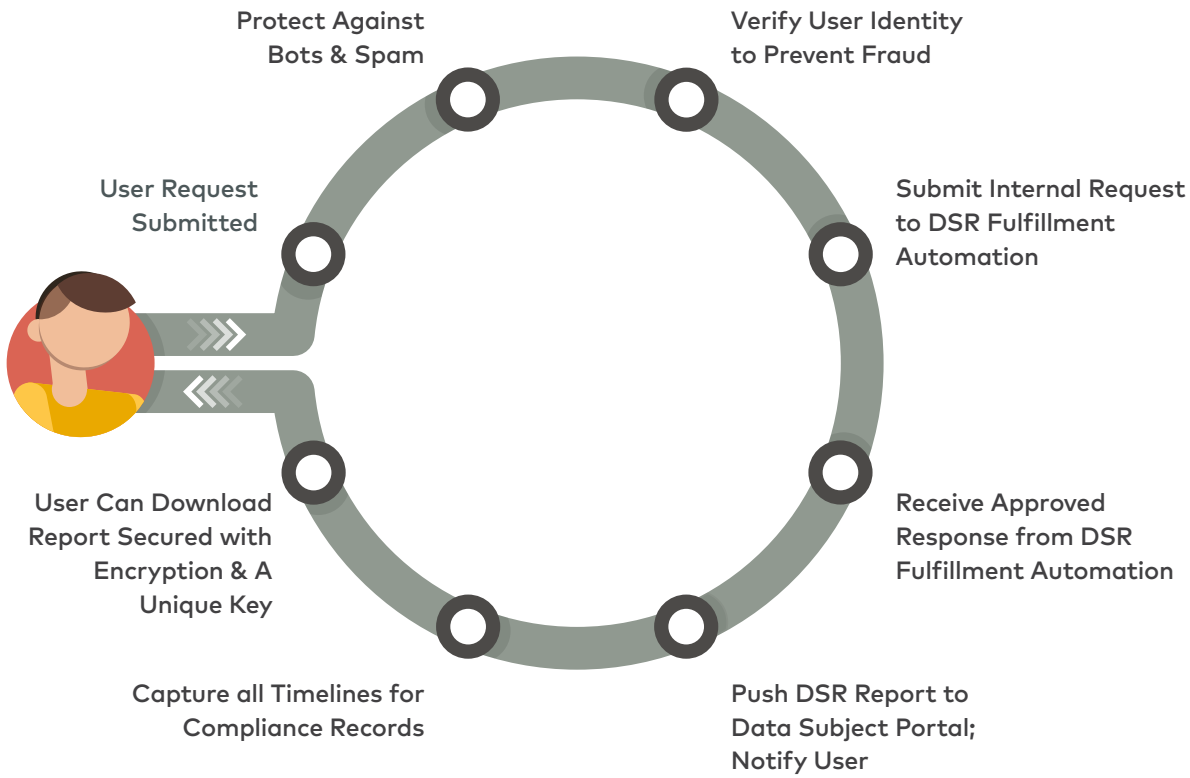
- Providing a means for subjects to submit DSRs. This could be in the form of emails, phone calls or online portals.
- Verifying the identity of the subject exercising their data rights.
- Providing all information to the subject in a report that they can download in a secure manner, while also ensuring that it does not create further sprawl of personal data along the chain of communication.
- Keeping an audit trail with timestamps of all communications, including the subject's data request time and fulfillment time.

PrivacyOps facilitates secure communication with subjects for making DSRs of various kinds.

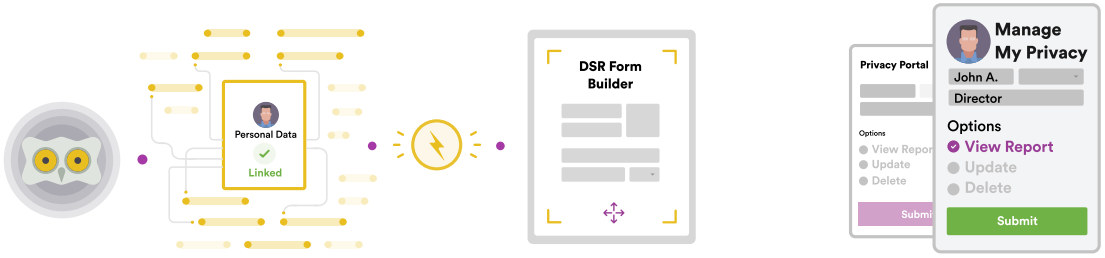
Secure communication includes:

- A cybersecure portal with which a subject can make DSRs. This portal must have the capability to detect attempts at fraud and spam against the enterprise. It must also detect malicious bots trying to spam enterprises and block them.
- An automated method for verifying the identity of various types of subjects.
- A cybersecure portal from which personal data can be shared with subjects, without relying on emails and other methods that can create further sprawl of sensitive data.

DSR Cybersecure Portal Flow



Data Subject Rights Robotic Automation



The cornerstone of DSR automation is AI-assisted automatic discovery of personal data and linking to its owners

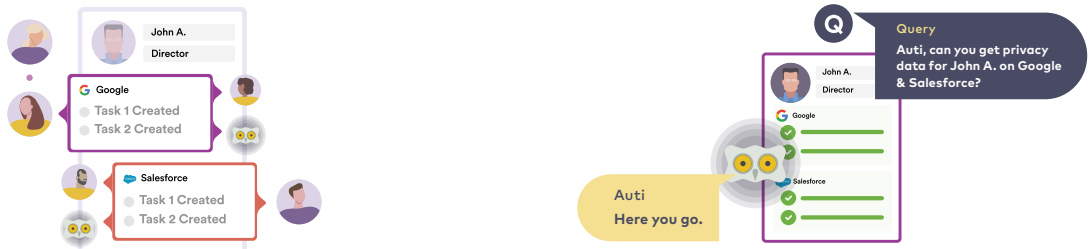
Build custom DSR form

Publish DSR forms & accept requests

Automatically locate & link subject's personal information

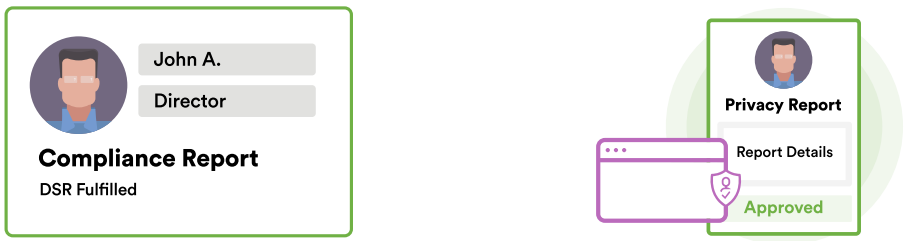
Robotic automation triggered

Verify subject's identity, create DSR ticket



Automatically create tasks & subtasks; invite stakeholders

The AI-powered bot assists in completing tasks & subtasks



DSR fulfilled, compliance report automatically created

Automatically share DSR report with subject, via cybersecure portal, after approval

CHAPTER 4

Internal Assessment Automation

Privacy compliance assessments are essential gap analyses against regulations, codes of conduct, and organizational standards of practice.

Organizations must identify gaps between existing controls and practices and what's expected by regulations or guidelines. The compliance requirements could be broadly applicable to the entire organization, or narrowly focused on a product, business unit or process within the organization. Organizations may have hundreds of internal systems that require internal assessment.

Privacy teams, business owners and auditors typically rely on word processing documents, spreadsheets and simple forms that result in work that is inefficient and hard to monitor.

The following are some of the challenges typical to internal readiness assessment practices:

- Collaboration over text docs or spreadsheets distributed to multiple teams is inefficient and hard to manage.
- Review, approval, and tracking of changes is not often institutionalized for regular (yearly) audits.
- Reminders and follow-ups to perform assessments must be done manually.
- Readiness analytics for a single assessment, and across all ongoing assessments for an organization, are difficult to compile.
- Evidence collected for all privacy assessments may float in different places, making it difficult to extract and compile when needed.
- Frequent changes and regulatory updates are difficult to keep up with.
- Assessment deadlines are difficult to monitor. Maintaining periodic updates incurs high operational overhead costs.
- Sharing compliance assessments with customers and partners is often a manual exercise using email and other insecure channels.

Privacy teams, business owners, and auditors must continuously deal with a complex regulatory landscape:

- Privacy laws are evolving continuously, with GDPR taking the limelight. Although GDPR has a high level of harmonization across the EU, its member states have introduced local data protection laws to supplement the baseline position, which in some cases, deviate from GDPR. This lack of uniformity makes it very difficult for organizations to keep track of changes and supplemental requirements.
- Many US states have or are expected to pass comprehensive privacy laws that are similar in spirit but may vary from one another in key areas. Tracking all these variations and interpreting their requirements becomes burdensome.
- Overall, privacy regulations are becoming more complex and difficult to interpret, resulting in a profusion of compliance programs.
- Brazil, India, Bahrain, Hong Kong, and many other countries have either passed new and comprehensive data protection laws, or materially have amended existing ones in line with GDPR.

PrivacyOps requires adopting a system-of-record, system-of-engagement, system-of-knowledge & system-of-automation for all internal assessments

To address these challenges with privacy assessments, PrivacyOps requires a system-of-record, a system-of-knowledge, a system-of-engagement, and a system-of-automation to ensure all stakeholders understand requirements, collaborate and complete assessments, and then share with external parties, all in one platform. Such a system must provide the following capabilities:

System of Record

A SYSTEM OF RECORD MAINTAINS:

- Privacy assessments completed by multiple teams within an organization.
- Evidence that documents compliance against individual requirements within each assessment.
- Approval and audit records to provide proof of compliance and operational integrity.
- An assessment archive for record management and regulatory compliance.

System of Knowledge

A SYSTEM OF KNOWLEDGE PROVIDES:

- A library of up-to-date and ready-made privacy assessment templates, based on country/state and their corresponding regulations—like GDPR, CCPA, etc.—all in one place.
- A knowledgebase of various global privacy laws and regulations.
- A library of custom assessment templates crafted and curated by an organization.
- Multi-regulation templates that ensure you comply with multiple regulations within a single audit.

System of Collaboration

A SYSTEM OF ENGAGEMENT AND COLLABORATION ENABLES:

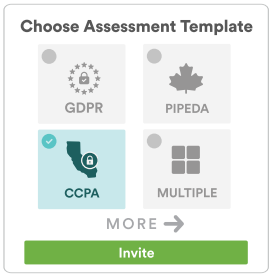
- Ease of assessment completion by stakeholders, by providing them the capability to assign various sections of the assessment to their internal subject matter experts.
- Built-in context-aware chat and discussions among subject matter experts to collaborate asynchronously to complete assessments.
- Comprehensive workflows to engage various stakeholders for input, review and approvals.
- Easy sharing of completed assessments with supporting documentation and evidence to businesses and partners.
- A robotic assistant that provides assistance in tracking assessment and providing answers to basic questions about internal assessments.

System of Automation

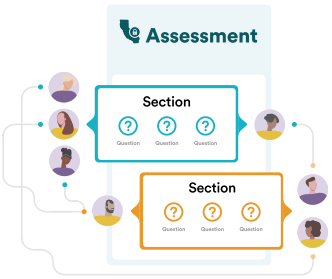
A SYSTEM OF AUTOMATION FACILITATES:

- Mapping of responses to multiple regulations, and assessing compliance against multiple regulations, with a single response.
- Autonomous reminders for assessment updates, based on time or the changes in underlying regulations.
- Regular privacy compliance posture reports shared with internal stakeholders.
- Analytics and tracking of assessment status and trajectory.
- An intuitive reporting dashboard so the governing authority within the organization understands the privacy readiness of the organization.

Internal Assessment Automation



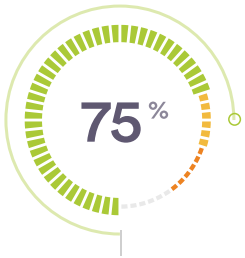
Initiate assessments



Invite stakeholders

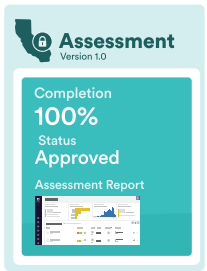
Stakeholders invite team members to contribute

Stakeholders collaborate on questions



Track progress in real time

Assessments reviewed



Assessments shared with external parties

Get insights about personal data from AI-powered bot

CHAPTER 5

Vendor Assessment Automation

A typical organization deals with hundreds or thousands of third parties, including vendors, partners and service providers. These third parties often have access to sensitive personal information of those within the enterprise.

Failure to adequately assess the privacy posture of such third parties exposes organizations to costly legal liabilities and reputational damage as well as regulatory penalties and even potential criminal liability. In addition, regulations such as GDPR clearly state that businesses—the data controllers—are ultimately responsible for ensuring that personal data is processed in accordance with GDPR. It also requires:

- **Having a written contract in place when appointing a data processor (vendor)**
- **Using only those processors who provide sufficient guarantees that they will meet the requirements of the related regulations, such as GDPR**

Therefore, unless a business demonstrates that all controls were in place and that it is "not in any way responsible for the event or actions giving rise to the damage," it will be held liable for any damage caused by non-compliant processors. This liability makes an effective third-party privacy risk assessment solution essential.

It is not practical to assess each vendor manually, therefore the need for an automated third-party assessment system is significant to minimize risk from both current and prospective vendors.

Some of the challenges associated with third-party management include:

- **Use of outdated, non-real-time techniques and tools such as Excel, Word, and PDFs**
- **Lack of consistency in assessment language and ratings due to a fragmented approach to vendor management using outdated tools and techniques**

- **Time-intensive and tedious manual processes requiring manual intervention and frequent follow-ups**
- **Lack of appropriate tools and expertise to process information gathered from vendors**
- **Difficulty ensuring all business owners are aware of the risks and continuously engaged in the process**
- **Lack of a single dashboard to assess the overall risk and a vendor's contribution to that risk**
- **Difficulty ensuring document management—agreements, contracts and other legal documents—are current and accessible**
- **Time-intensive and tedious monitoring of the vendor's security posture including breach notification if the vendor is involved in a security incident**

PrivacyOps requires adopting a system-of-record, system-of-knowledge, system-of-engagement, and system-of-sharing for all vendor assessments

To address the above challenges with privacy assessments, PrivacyOps requires a system-of-record, a system-of-knowledge, a system-of-engagement, and a system-of-automation to bring all vendors together in one place, to communicate privacy needs and complete assessments, with one platform. It must provide the following capabilities:

System of Record

A SYSTEM OF RECORD MAINTAINS:

- Lists of vendors and details of each vendor. It supports the bulk importing of hundreds or thousands of existing vendors for privacy assessments, as well as adding new vendors one at a time.
- Privacy assessments completed by all vendors.
- Documents and contracts provided by vendors related to privacy assessments. All attachments provided by vendors as supporting documents and pieces of evidence, along with assessment. These documents typically include data protection agreements, SOC2 reports, vulnerability assessments, etc.
- A system to retire and archive vendors. It documents and tracks data destruction activities and deactivation workflows.

System of Knowledge

A SYSTEM OF KNOWLEDGE PROVIDES:

- A library of up-to-date and ready-made privacy assessment templates, based on country/state and their corresponding regulations—like GDPR, CCPA, etc.—in one place.
- Regular updates to address changes in various global privacy regulations.
- A library of custom assessment templates crafted and curated by the organization.
- Multi-regulation templates that let you comply with multiple regulations within a single audit.

System of Engagement and Collaboration

A SYSTEM OF ENGAGEMENT AND COLLABORATION ENABLES:

- Seamless invitations to hundreds or thousands of vendors to complete selected privacy assessments in one place.
- Organizations to communicate with vendor assessment owners within the platform, instead of over insecure communication tools.
- Ease of assessment completion by vendors, by providing them the capability to assign various sections of the assessment to their internal subject matter experts.
- Collaboration among subject-matter experts with built-in context-aware chat platforms that let them work asynchronously to complete assessments.
- Comprehensive workflows to engage various stakeholders for input, review and approvals.
- Tracking assessments through a robotic assistant that provides answers to basic questions about various vendor assessments.

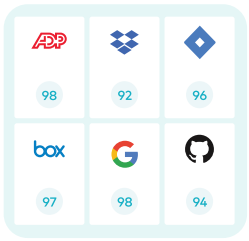
System of Automation and Insights

A SYSTEM OF AUTOMATION DELIVERS:

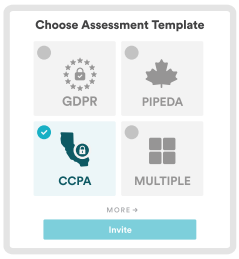
- Systematic follow-ups with vendors to complete privacy assessments and provides necessary documents and evidence.
- Mapping of responses to multiple regulations, and assessing compliance against multiple regulations, with a single response.
- Ease of assessment updates for vendors; automatic reminders for assessment updates, based on time or any change in underlying regulations.
- Creation of regular privacy compliance posture reports for all regulations for sharing with internal stakeholders.
- Analytics and tracking of vendor assessment status and trajectory.

Vendor Assessment Automation

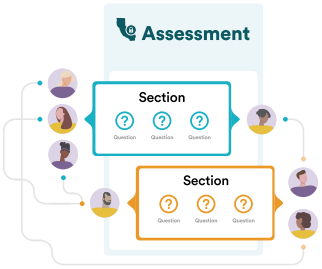
Discover & upload vendor list



Review vendor privacy scores



Pick regulations for vendor assessment

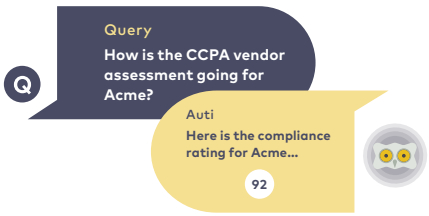


Vendors invite their subject matter experts

Vendors get immediate access

Invite vendors to complete an assessment

Subject matter experts provide inputs & evidence



Ask AI-powered bot about progress on assessments

Vendor responses received & recorded

Compare insight & analytics across vendors

Get regular updates on assessments

CHAPTER 6

Vendor Privacy Risk Monitoring

Companies are increasingly dependent on third parties for processing information. In many cases, this includes personal information, which makes organizations responsible for the personal data managed by their third parties.

Regulations such as GDPR place the responsibility of protecting subjects' personal data completely on the organizations collecting personal data and processing that data through third parties. Both controllers and processors must have confidence that all of their third-party partners comply with privacy regulatory requirements. Also, most regulations mandate ongoing, periodic assessments to ensure compliance guidelines are being followed.

In addition to getting a privacy assessment completed by a vendor, and gathering evidence related to the vendor's compliance, it is also be beneficial to obtain an independent assessment of the privacy risk posed by a vendor. This allows organizations to develop an effective strategy for data protection, risk management and compliance. Such an independently created privacy rating of an organization, allows customers to understand the privacy and data posture of the vendor across the following multiple risk factors.

Data Protection

Data protection comprises the processes implemented by the vendor to protect the data that it collects, processes and disseminates. This includes not just the processes and technologies the vendor implements to protect data but also the political and legal underpinnings surrounding the data. It includes risks around:

Data Collection

Addresses risks around the vendor's data collection processes including the richness of notification messages, which should include reasons for collecting data and the categories of personal data collected. It also addresses the ability to collect explicit consent from users and the special handling of underage consumers.

Data Storage

Addresses risks around the vendor's data storage and data retention capabilities to understand how effective they are in keeping sensitive data safe and secure. Key capabilities analyzed should include transport level encryption, encryption at rest, access control mechanisms, fault tolerance, retention and backup capabilities, and forensic event logs for effective alerting, reporting, and policy actions.

Data Sharing

SaaS, IaaS and Platform as Service (PaaS) vendors acquire volumes of data about their customers which could be misused, leaked or sold to other third- parties, increasing the risk to the business.

It's important to review and understand how the data is analyzed or monetized by the vendor. Other critical risk factors to analyze are the financial incentives baked into contracts and agreements to collect and sell PII information.

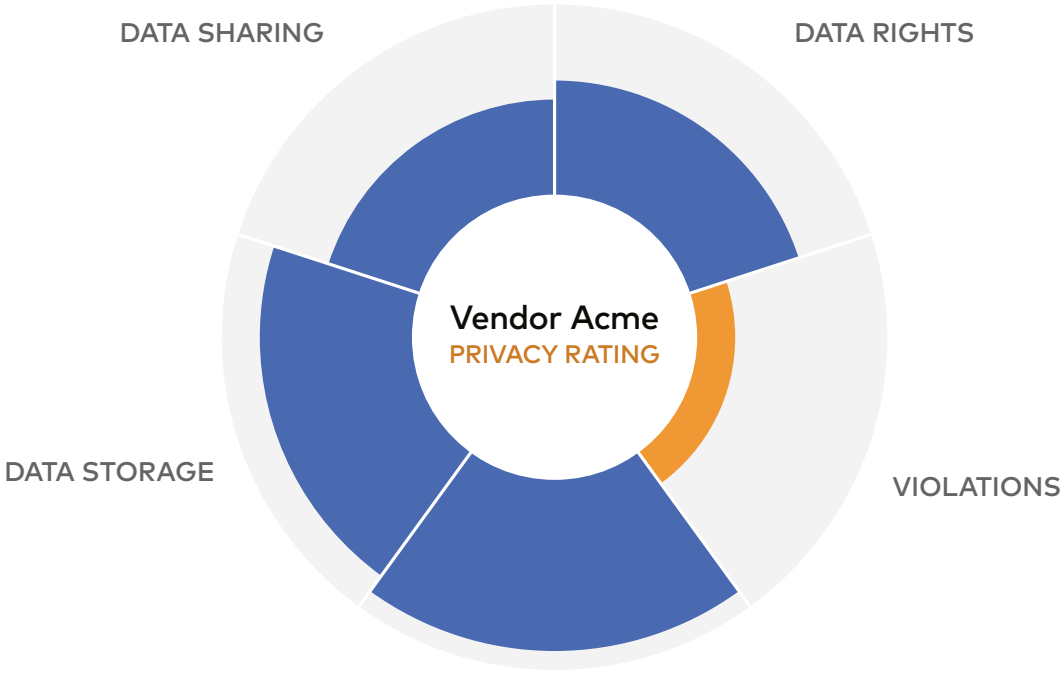
Privacy Violations

Good indicators of a vendor's privacy health comes from the number of incidents resulting in a fine from a regulatory body and the number of data breaches experienced by the vendor. Few or no violations indicate a good security posture.

Businesses are responsible for vendors who process personal data on their behalf as a processor or service provider and any fines and breaches experienced by the vendor also indirectly harm the reputation of the business itself. Knowing a vendor's track record in maintaining its cyber security posture is essential to reduce the company's risk exposure.

Respect for Consumer Data Rights

The ability of a vendor to satisfy customer data requests for the data it collects and processes is a good indicator of the maturity of its privacy program. Responsible vendors incorporate best privacy practices into their design and development processes and offer tools and solutions to satisfy customer data requests within their SaaS products. These qualities are of significant operational value to the business. Assessing the vendor's maturity in handling consumer data rights requests is an essential part of vendor assessment.



Scoring System for
Vendor Privacy Ratings

CHAPTER 7

Consent Lifecycle Management

Individual consent is a core principle that shows up prominently in all privacy directives and regulations. Consent is an expression of will, with which the data subject authorizes (or withdraws authorization for) the processing of personal data.

It puts individuals in control of how their personal data is collected and used. Although consent is only one of six legal bases for processing personal data, it's one of the most well-known approaches by which businesses establish trust while processing personal information.

There are Many Challenges to Effective Consent Management

The first challenge involves the process of notification and consent capture.

In principle, all privacy regulations agree that consent must be freely given, specific, informed and unambiguous. For consent to be informed and specific, the data subject must at least be notified about the controller's identity, what kind of data will be collected and processed, how it will be used, and the purpose of the processing operations. While businesses are building new capabilities into their forms, mobile apps, and websites to enable consent capture, having a solution for notification and consent capture immensely simplifies this requirement.

The second challenge involves the proliferation or sharing of captured consent.

Websites and businesses collect and store identifiers such as IP addresses, device IDs, location data, and cookies, all of which are now considered personal data. This information is shared or leaked to various advertising and marketing platforms to provide value-added services. For instance, under GDPR, every platform involved in this process must notify and obtain consent from the user to collect and process their data. Consent propagation must be supported and managed.

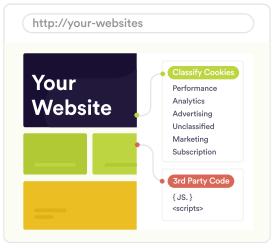
The third challenge encompasses associating a given consent to a specific user or identity.

This is easier said than done, since most businesses have personal data scattered throughout multiple systems and silos, with different identities for the same user, using different processes, within varying environments. The enterprise-wide view of this data so essential to effective consent management is difficult to achieve and maintain.

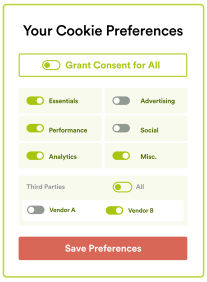
The fourth challenge concerns governance.

Most businesses undertook a flurry of consent capture and re-consent efforts to meet GDPR deadlines, but ended up with solutions that act as static databases for consent frameworks and preferences. Without the ability to link consent to identities, consent is once again scattered around silos with multiple instances of consent for each user. This makes opt-out and consent withdrawal decisions very difficult to implement across an organization. Therefore, operationalizing consent management is a critical requirement for consent management solutions.

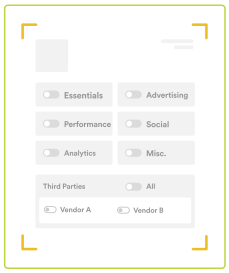
Consent Lifecycle Management



Scan websites to detect and classify dropped cookies

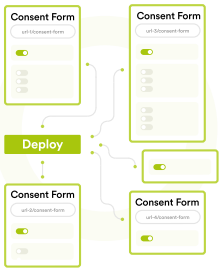


Build customized consent collection methods

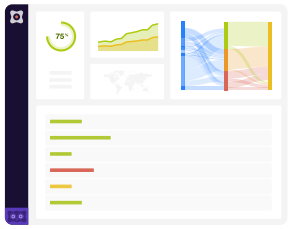


Customize collection end point

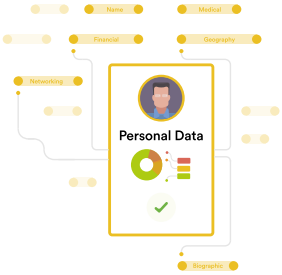
Apply intelligent methods to meet compliance requirements



Rapidly deploy consent collection points



Never miss collection of consent



Link consent to user identities and PD categories

Visualize consent at user and organizational levels

Alerts issued if PD is collected without consent

An automation-centric PrivacyOps framework addresses the cited challenges of consent management by providing the capabilities outlined in the following sections:

Policy Notification and Collection of Consent

The process of effective consent management always begins with the right notifications. First, users must be informed that their personal data is being processed. Detailed information about the scope of data processing must be included in the Privacy Policy, in a pop-up notice, or in both. Users must be empowered to decide if they agree to the specific purpose of processing. Consent must be captured and consolidated.

KEY CONSENT MANAGEMENT CAPABILITIES INCLUDE:

Privacy Center

- **Creates, maintains, and publishes an organization's privacy mission statement while engaging with their customers to articulate how and why they collect and process their personal data**
- **Highlights their commitment towards privacy to build trust**

Privacy Policy Builder

- **Builds and publishes an external-facing privacy policy**
- **Builds and publishes a global or personalized cookie policy for every website managed by an organization**

Website Scanning and Cookie/Form-based Consent Management

- Periodically scans websites to discover which cookies are dropped through the website and includes those in cookie consent banners
- Provides tools to integrate cookie consent capture and management into web pages
- Provides tools to integrate form-based consent capture into web pages

Bulk Consent Import

- Facilitates the manual import of consent data
- Allows third-party integration through APIs for consent import

Visualization

- Visualizes 3rd-party assets deployed on enterprise websites

Propagation Management

The PrivacyOps consent framework simplifies the notification, collection, and propagation of consent to approved 3rd-party solutions to meet business objectives. Key capabilities should include:

Adherence to the Interactive Advertising Bureau (IAB) Framework

- Consent banner notifications that allows users to select companies with whom the publisher can share data
- Enables websites to pass users' consent decisions down the supply chain

Improve Accessibility to Consent Data

- Push (webhooks) or Pull (API) based flexibility to make consent accessible to internal business applications so that they can make the appropriate decisions while processing personal information

Map and Correlate

PrivacyOps helps to collect, normalize and aggregate consent from multiple and varied sources.

Visualize Consent Actions in Dashboards for Analysis. This Includes:

- Cookie consent
- Form-based consent
- Consent propagation
- Bulk import of consent
- API based consent ingestion

Correlate Multiple Consent Actions by the Same Data Subject

- Link consent to identity
- Provide an enterprise-wide view of consent based on identity and identity categories (customers, employees, vendors, temporary users, etc.)

Evaluate Policies From a Central Location

- Detect data that is collected or retained without explicit consent

Track, Govern and Manage Consent

PrivacyOps enables companies to comply with a consumer's request to opt-out or withdraw consent of the processing or sale of their personal data

Consent Management Portal

- Tools to manage consent globally through a hosted page; ability to propagate decisions to internal business applications
- Cookie consent through on-demand consent banner

Integrate Consent Management into Data Maps and Business Process-Flow Diagrams

- Incorporate consent management into data maps
- Incorporate consent decisions into records of processing activity to satisfy GDPR Article 30 requirements
- Single Identity Dashboard
- Visualize consent for each data subject in a single, comprehensive dashboard which includes visualization of PD processed within an organization for that user and consent validity

Automation

PrivacyOps helps automate and orchestrate most of the mapping, correlation and governance activities associated with consent management.

AI & BOT-ASSISTED PRIVACYOPS CAN:

- Scan websites to automatically discover and categorize cookies.
- Assist in updating the privacy policy or cookie policy and publish it in a hosted, customizable privacy portal
- Automatically map and correlate consent actions to a unique identity or data subject
- Assist in search and visualization of consent for a particular identity, location, datastore, etc.
- Automatically propagate consent (grants and withdrawals) to business applications
- Automatically keep an audit trail of all the steps taken to collect and manage consent
- Automatically integrate consent reporting into data subject rights tickets to indicate how consent was collected for particular PD processed by an organization
- Automatically integrate consent reporting into data maps and seamlessly ensure that it makes it into Article 30 reports

CHAPTER 8

Data Mapping

Data mapping is the system of cataloging the data collected by an organization, how that data is used, stored and processed, and how that data travels within and beyond an organization.

A fundamental requirement of any privacy regulation is understanding what personal information is being collected, how it is processed and where it is stored. This sets the baseline from which to assess privacy risks, ensure the safekeeping and fair use of personal data, and handle requests from data subjects and regulators in a timely fashion. In addition, privacy laws such as GDPR directly mandate data mapping requirements in multiple articles of the regulation:

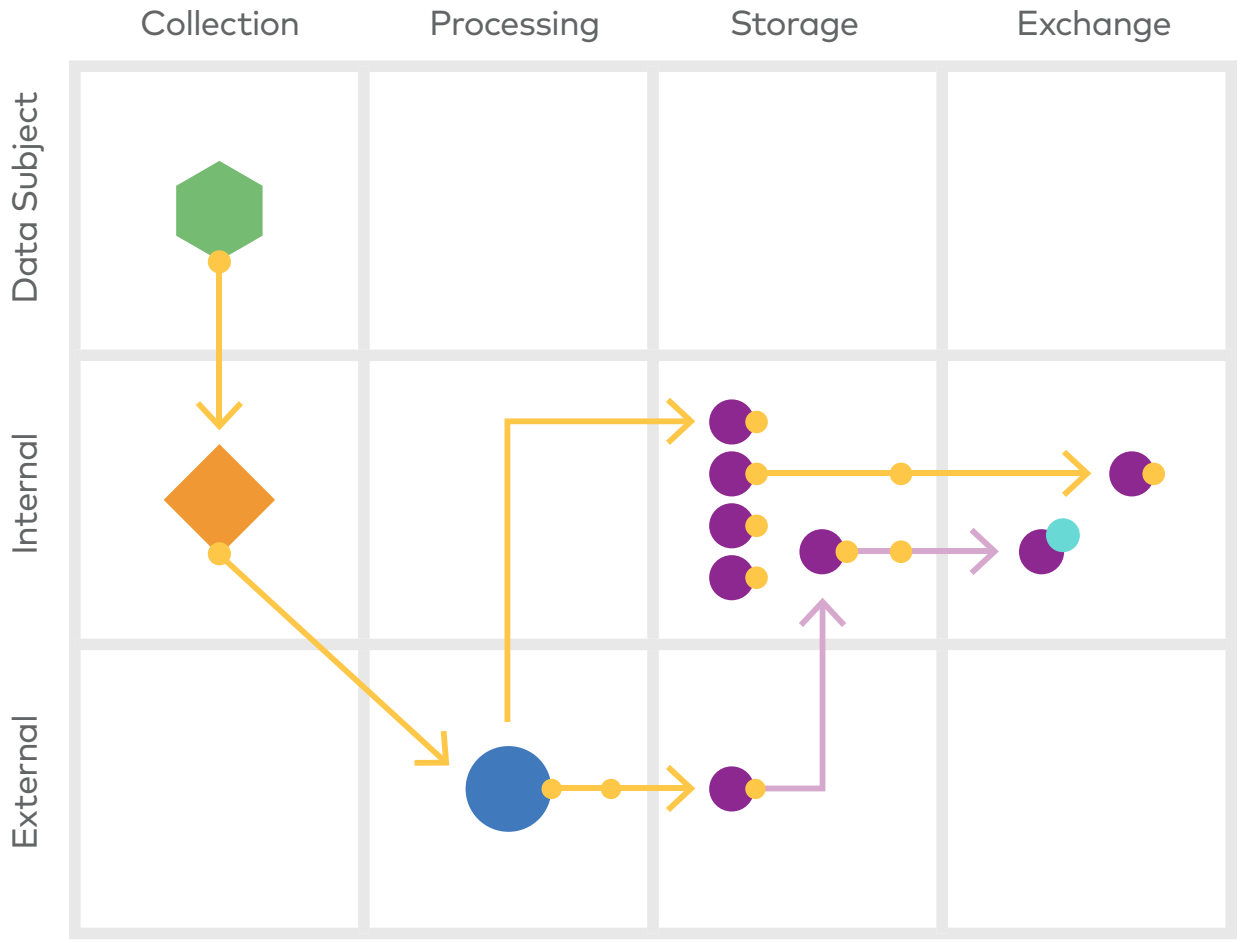
GDPR Article 30—Records of Processing Activities

- Each controller shall maintain a record of processing activities under its responsibility
- Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller
- The records shall be in writing, including in electronic form
- The controller or processor shall make the record available to the supervisory authority upon request

GDPR Article 35—DPIA

- Mandates that any processing of personal data using new technologies in a way that puts data subject rights at risk must undergo a Data Protection Impact Assessment (DPIA)
- Mandates that a data map act as the foundation for a DPIA by satisfying 2 out of 6 steps to carry out an effective DPIA, mainly:
  1. Describing the information flow
  2. Identifying privacy and related risks

Unfortunately, most organizations have a siloed and broadly scattered application landscape. There are multiple data collection and processing elements combined with in-house and cloud-based application and storage infrastructure, with highly fluid data sharing and processing agreements in place. With more than 80% of enterprise workflows now moving to the cloud, organizations are finding it hard to document and track the flow of information within their vendor's cloud infrastructure.



In most organizations, data catalogs and maps are hidden away in outdated spreadsheets, Powerpoint or Visio diagrams, making it impossible to bring clarity to this gigantic mesh of interconnected interfaces, systems, and processes.

Also, without a collaborative documentation and knowledge sharing environment, it is typical for business process knowledge to get locked up in the minds of subject matter experts, making it nearly impossible to build and maintain an accurate record of data. A good data mapping solution supports an organization's privacy compliance requirements by allowing it to collaboratively gain full visibility into the flow and control of personal data—not just within an organization but also outside its boundaries.

To address the above challenges with data mapping, PrivacyOps requires a system-of-record, a system-of-knowledge, a system-of-engagement, and a system-of-automation to bring all your subject matter experts (SMEs) into one place to document and track the flow of information, in one platform. It must provide the following capabilities:

System of Record

A SYSTEM OF RECORD MAINTAINS:

- **Information flow within an organization, between organizations (processors, contractors, suppliers), outside an organization and data flow across countries**
- **Extensive metadata for every element within a data map including data type, data format, location, accountability, access list, etc.**
- **Definitions of all PD attribute types handled by the data map element**

System of Knowledge

A SYSTEM OF KNOWLEDGE PROVIDES:

- An expandable, organization-centric icon library
- Allows users to define a components once and use it within multiple data maps or business process flow diagrams
- Data maps that users can clone and enhance, making the process efficient and extensible
- An easy to understand, visual artboard from which users can describe the information flow
- A portal that ensures the right users and SMEs create, collaborate and provide feedback on information flows
- Intelligent connection options that track PD attributes along with the information flow
- An inventory for all business flow assets
- An interface of the system-of-record to glean insights into data flows by capturing all the characteristics of a flow including direction, properties, restrictions, and ownership
- Reduction of uncertainties in business flows where typically one or more subject matter expert would need to be consulted
- Support for business and organizational decision-making capabilities through a combination of business flow records, component metadata, system-ownership and system-generated insights including data classification and privacy alerts

System of Engagement and Collaboration

A SYSTEM OF ENGAGEMENT ENABLES:

- Mapping of complex data flows and business process diagrams on a flexible and collaborative artboard
- Working with multiple subject-matter experts and process/solution owners seamlessly within a single, collaborative data map
- Messaging capabilities to communicate with and to invite collaborators
- Working with teams on any device across multiple platforms and geographies
- A collaborative, easy to use environment that ensures that the data map is always up to date through automation, notifications and policy alerts

System of Automation and Insight

A SYSTEM OF AUTOMATION DELIVERS:

- Automated data maps created through metadata ingestion
- Automatic scanning and classification of data in hundreds of locations to populate properties for map elements
- The use of PD attributes discovered during live data scans as component metadata within data maps
- Periodic re-scans to ensure the data is always up to date
- Automatic monitoring of map elements and process flows for compliance violations such as data collection without consent, improper access privileges, etc.
- Breach impact analysis as it applies to data flows and business processes
- Policy-based alerts to identify weak security processes and non-compliance to legal or regulatory requirements
- Consent tracking at each stage of the data flow and highlights data that may have been collected, stored or processed without consent

NOTES

CCPA

CALIFORNIA CONSUMER
PRIVACY ACT

GDPR

EU GENERAL DATA
PROTECTION REGULATION

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The California Consumer Privacy Act (CCPA) goes into effect January 1, 2020.

Considered one of the broadest privacy laws in the United States, CCPA provides California residents with the ability to control how businesses process their personal information. Businesses not only have to implement a number of CCPA-specific requirements while implementing their privacy programs, but also stop selling consumer data upon request. Businesses also have to honor requests from California residents to access, delete, and opt-out of sharing or selling their information.

Who Needs to Comply?

Any for-profit business that collects information for California residents and meets at least one of the following thresholds must comply with the CCPA:

- ☑ **Revenue is $25 million or greater;**
- ☑ **Buys, receives, sells, shares the personal information for 50,000+ consumers**
- ☑ **Generates at least 50% of its annual revenue from selling personal information.**

Nonprofits and smaller companies that don't meet the revenue thresholds, and/or organizations that don't collect/share/sell large amounts of personal data from California residents won't have to comply as long as they don't have and affiliate with a brand that is covered under the CCPA.

Extra Territorial Applicability of CCPA

CCPA applies to for-profit companies established in California and entities that indirectly qualify as doing business in California, including parents and subsidiaries of companies established in California.

Organizations located outside of California are also subject to the CCPA if the business transacts with California residents and meets any of the threshold requirements.

Consumer Privacy Rights

Under the CCPA, consumers have new and stronger data privacy rights. They include:

RIGHT TO KNOWLEDGE

Consumers have the right to request and obtain from businesses information about:

- The personal data the business collects about them
- How that personal data will be used
- If and with whom that personal data is shared or sold to

RIGHT TO BE FORGOTTEN

Businesses must delete all personal data they hold about a consumer at the consumer's request. The only exceptions allowed are:

- Data that is retained to complete a consumer-requested transaction
- Data that is retained for specific research purposes
- Data for limited analytical use and
- Data needed to comply with regulatory and contractual requirements.

RIGHT TO CONTROL ACCESS TO INFORMATION

Consumers have the right to opt of the sale of their personal data to third parties.

What Does it Mean for Businesses?

Despite being a state law, CCPA will impact businesses globally. Business must:

KNOW THEIR DATA

Catalog and maintain an inventory of all data stores, locations, third parties, partners, operations, business processes and applications collecting and processing personal data of California residents.

PROVIDE APPROPRIATE DISCLOSURES AND UPDATE CONSUMER NOTIFICATIONS

At every personal data collection point, inform consumers about

- Their rights under CCPA
- Categories of personal data collected
- How the collected personal data will be used
- Who it will be shared with
- Categories of personal data that have been shared with third parties in the past 12 months

SATISFY CONSUMER DATA RIGHTS REQUESTS

Address consumer data rights requests after verifying/authenticating the identity of the consumer, in a timely fashion which includes:

- **Right of access**—includes the ability to view all the personal data the company has about them
- **Right to erasure**—ability to delete all the personal data the company has about them
- **Right to opt-out**—ability to opt-out of the sale of their personal data

IMPLEMENT OPT-IN CONSENT FOR CHILDREN'S DATA

Business must implement explicit opt-in consent for sale of personal data belonging to children under 16. For children between 13 and 16 years of age, consent can be collected directly from the child. For children under 13, opt-in consent must be obtained from a parent or guardian.

IMPLEMENT OPT-OUT MECHANISMS

Place an easily accessible link titled "Do Not Sell My Personal Information" on their homepage.

MANAGE VENDORS

Identify vendors or third parties that handle or process a California resident's personal data on behalf of the business or sell personal data to the business. Review and manage contractual obligations to ensure personal data is handled in compliance to CCPA requirements.

EVALUATE THEIR SECURITY POSTURE

Periodically review their security and privacy policies and procedures and data protection mechanisms to ensure all the necessary controls are in place to protect California residents' personal data.

Penalties

CCPA authorizes California's Attorney General (AG) to seek civil penalties and entitles California residents to a private right of action they suffer a data breach or data theft.

NONCOMPLIANCE PENALTIES

- Unintentional penalties for noncompliance range from $2,500 per violation if the violation is found to be unintentional and $7,500 per violation if found to be intentional.

DATA BREACH PENALTIES

- If personal information is exposed as a result of a data breach, consumers can initiate civil action lawsuits against an organization resulting in penalties between $100 to $750 per consumer, per incident or greater if the actual damages exceed $750.

Definition of Personal Information Under CCPA

The definition of Personal Information (PI) under CCPA is much broader than GDPR or other privacy laws in the United States.

CCPA defines personal information as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This includes a wide range of standard personal data attributes including financial and contact information and "unique personal identifiers" such as device identifiers and online tracking technologies.

EU GENERAL DATA PROTECTION REGULATION

The EU General Data Protection Regulation (GDPR), effective as of 25th May 2018, replaces EU Directive 95/46/EC: the Data Protection Directive and all its local variants and is valid in every country within the EU.

Who Must Comply

Any organization that processes personal data within the European Union falls under the scope of the GDPR.

This includes non-EU organizations offering products or services to individuals in the EU irrespective of where the data processing is done. The products or services offered by an organization could be paid or free, GDPR applies uniformly across these organizations. Under GDPR, organizations are categorized as *controllers* and *processors*. A *controller* determines what happens with the personal data and how data is processed. A *processor* processes the data solely on behalf of the controller.

Extraterritorial Applicability of GDPR

The territorial scope of GDPR has been broadened so that its rules now also apply to data controllers and processors outside the EU who must comply with EU data protection obligations when they process data from individuals or data subjects in the EU.

This includes any organizations that offer free or paid products and services or monitors the behavior of individuals in the EU.

Citizenship does not affect the territorial scope of GDPR. If a product or service is offered within the EU, then the data processing must comply with the GDPR, whether or not the company is physically located in the EU. Therefore when an individual leaves the EU to a non-EU country, they are no longer protected by the GDPR. In such cases, the individual's data rights and freedoms are dictated by local laws and regulations.

Data Subject Privacy Rights

Under the GDPR, consumers have new and increased data privacy rights. This includes:

RIGHT TO ACCESS PERSONAL DATA

Data subjects have the right to access the data collected on them by a data controller. Along with a confirmation that the data subjects personal data is being processed and a copy of the personal data, the data subject is entitled to additional information around the data processing, including:

- Purposes of processing
- Categories of personal data concerned
- Recipients or categories of recipients the personal data is disclosed to
- Retention period for storing the personal data
- Information about the source of the data
- Existence of automated decision-making (including profiling)
- Safeguards in place to protect data transfer activities

RIGHT TO DATA PORTABILITY

A data subject can request that their personal data file be sent electronically to a third-party or handed over to the data subject. Data must be provided in a commonly used, machine- readable format, if doing so is technically feasible.

RIGHT TO ERASURE

Also referred to as the right to deletion or the right to be forgotten–this allows a data subject to stop all processing of their data and request their personal data be erased.

RIGHT TO RECTIFICATION

Data subjects have the right to request modification of their data, including the correction of errors and the updating of incomplete information.

RIGHT TO RESTRICT DATA PROCESSING

Data subjects, under certain circumstances, can request that all processing of their personal data be stopped.

RIGHT TO OBJECT

When a data controller denies their request to stop data processing, a data subject has the right to object to the denial.

RIGHT TO REJECT AUTOMATED INDIVIDUAL DECISION-MAKING

Data subjects have the right to refuse the automated processing of their personal data to make decisions about them if that significantly affects the data subject or produces legal effects.

RIGHT TO BE NOTIFIED

Data subjects must be informed about the uses of their personal data in a clear manner and be told the actions that they can take if they feel their rights are being impeded.

What Does it Mean for Businesses?

Despite being a law, GDPR impacts businesses globally. Business must:

APPOINT A DATA PROTECTION OFFICER

Businesses must appoint a Data Protection Officer (DPO) when they act as public authorities, monitor data subjects on a large scale and process special categories of data. The DPO is a special role that supervises and offers necessary advice in matters related to privacy, data protection regulations and procedures. The DPO also monitors compliance with regulations and acts as the main point of contact with data subjects and supervisory authorities for all data protection matters.

KNOW THEIR DATA

Catalog and maintain an inventory of all data stores, locations, third parties, partners, operations, business processes and applications collecting and/or processing personal data of EU data subjects or individuals.

UNDERTAKE AND MAINTAIN DATA PROTECTION IMPACT ASSESSMENTS

GDPR expects organization to proactively include data protection in the design of systems, for example, privacy by design, rather than act in retrospective. Controllers must initiate Data Protection Impact Assessments (DPIA) depending on the nature of data processing activity and the risk it imposes on the data that is handled.

MANAGE VENDORS (PROCESSORS)

A processing agreement is necessary when another party (processor) is involved in the processing of personal data for which an organization (controller) determines the means and purposes. Under these circumstances, the controller must establish processing agreements and monitor vendors for compliance.

OBTAIN EXPLICIT CONSENT BEFORE PROCESSING DATA

Organizations must ensure their public-facing privacy-policies and notices are concise and clear. Organizations must obtain freely given, informed, explicit consent before undertaking any data processing activity.

SATISFY CONSUMER RIGHT TO DATA ACCESS AND PORTABILITY

Address data subject rights requests after verifying and authenticating the identity of the data subject. This includes the right to data portability which allows data subjects to request copies of their data in machine- readable format.

SATISFY CONSUMER RIGHT TO BE FORGOTTEN

Ensure that upon request the organization erases the data subject's personal data, ceases further dissemination of the data, and notifies applicable third parties, including processors, to halt processing of the data.

IMPLEMENT PARENTAL OPT-IN CONSENT FOR CHILDREN'S DATA

Organizations must implement explicit parental opt-in consent before processing personal data belonging to children under 16. Individual member states may choose to set this age threshold as low as 13 years for minors.

KNOW THEIR RESPONSIBILITIES AS PROCESSORS

Processing must always be based on formal, documented instructions from the controller. Processors must:

- Demonstrate GDPR compliance of processing activities to controllers and supervisory bodies
- Engage other processors only with written approval from controllers
- Communicate any special data transfer regulations they are subject to
- Assist controllers in fulfilling data subject rights requests
- Implement security controls to ensure data protection as outlined by the GDPR

KNOW HOW TO RESPOND TO A DATA BREACH

Businesses (controllers and processors) must take every possible measure to eliminate the risk of data breaches. In the event of a data breach, businesses must notify supervisory bodies, controllers (if the business is a processor) and individuals impacted by the data breach within 72 hours.

Penalties

GDPR imposes substantial fines for non-compliance. Fines up to €20 million or 4% of annual global turnover could be imposed with fines applying to both controllers and processors.

Definition of Personal Data Under GDPR

The scope of personal data under GDPR is broad, however, the GDPR is only applicable when personal data is processed.

Personal data is data by which a natural person can, directly or indirectly, be identified. This includes *regular* personal data such as names, addresses, emails, device information such as IP addresses or device IDs and 'special' categories of personal data such as genetic data and biometric information.

GDPR also applies when data is indirectly traceable to a person. Pseudonymized or anonymized data should be treated like personal data, however, pseudonymization is considered an acceptable form of securing personal data under GDPR.

Anonymized data is considered exempt under GDPR only if the data is encrypted, the key destroyed and therefore all data lineage traceable back to a person has been destroyed (i.e., the encryption is irreversible).

PrivacyOps

PrivacyOps is the combination of philosophies, practices, cross-functional collaboration, automation and orchestration that increases an organization's ability to comply with a myriad of global privacy regulations, reliably, and with greater speed.

PrivacyOps evolves an organization from traditional manual methods across various functional silos, to full automation, in a cross-functional collaborative framework, for most aspects of privacy compliance. The reliability and responsiveness of a PrivacyOps system enhances an organization's trust equity, making any organization more trustworthy with sensitive personal data.

PrivacyOps.com

ISBN 978-1-7333560-0-8