elastic

Using Elastic to power compliance with global privacy laws

Executive summary

To operate successfully in the modern digital world, organizations are focusing on data, especially its role in AI. In response, an explosion of privacy laws and regulations is reshaping the global business landscape. Keeping up with these regulatory developments isn't just about reducing and mitigating risk; it's a critical and powerful market differentiator, where compliance with the rapidly changing legal and regulatory privacy landscape can also boost customer trust, power financial growth, and strengthen operational resilience.

This white paper introduces essential concepts in data privacy law and demonstrates how organizations can deploy Elastic's powerful platform to not only meet the applicable personal data requirements, but operationalize them with speed, efficiency, and confidence. We will outline the six foundational privacy principles that are broadly applicable to data privacy regulations around the world and map these to Elastic's platform solutions, helping organizations turn data privacy from a compliance obligation into a competitive advantage.

Please note: This white paper is provided for informational purposes only and is not intended to constitute legal advice. Please consult your own legal counsel for legal advice.

Background and global privacy law primer

Global privacy laws create increasingly complex challenges for organizations that collect personal data. With personal data widely regarded as one of the most valuable commodities in the world, compliance with privacy laws can be a significant business driver for enterprises and failure to comply can significantly impede a company's growth.

As organizations collect more personal data, finding a scalable solution to manage and protect that data becomes increasingly critical to demonstrating accountability and building a positive reputation as a trusted vendor in an increasingly privacy-conscious world.

While there are distinctions between various privacy laws, many of them share certain overarching principles.

Key privacy laws include:

- The EU's General Data Protection Regulation ("GDPR") and its United Kingdom analog
- US state privacy laws like the California Consumer Privacy Act ("CCPA")
- The Brazilian General Data Protection Law ("LGPD")
- Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA")
- Japan's Act on the Protection of Personal Information ("APPI")

The flexibility and scale of Elastic's platform offering empowers organizations to navigate and manage compliance with these various and complex legal requirements.

Personal data

Gone are the days when the concept of “personal data” was limited to obvious identifiers such as full names, email addresses, government identifiers, and phone numbers. These days, privacy laws around the world define personal data broadly to capture any information that can be associated with a specific device or individual.

A good rule of thumb would be to assume that privacy laws likely apply if information can be tied to a unique identifier of a person. With smartphones, IoT devices, and other computing devices ubiquitous in everyday life, the collection of personal data has ballooned across organizations of all industries, creating a pressing, undeniable need for products and services that enable organizations to confidently manage the processing of such data.

Controllers and processors

Privacy laws worldwide typically impose different — but often overlapping — obligations on organizations depending on whether they act as a “controller” or a “processor” of personal data.

- **Controllers** (also called “businesses” under the CCPA) control the purposes and means of processing personal data. They are the entities that get to make independent decisions about what personal data they will collect and how they will process it.
- **Processors** (also called “service providers” under the CCPA) provide services to an upstream controller (or sometimes another processor) and are only permitted to process personal data strictly in accordance with the controller’s instructions for purposes of providing services to the controller.

While different obligations apply to controllers and processors, compliance in each role requires understanding the types of personal data being processed and being able to locate personal data in a targeted, scalable, and efficient fashion.

Most privacy laws around the globe also empower individuals to exercise certain rights to their data, such as access, deletion, and correction. With relatively short windows to respond, using a platform like Elastic to efficiently sift through unstructured and structured datasets will not only help streamline compliance but also reduce risks of regulatory investigations and civil litigation.

Foundational privacy principles

Global privacy laws are often based on foundational privacy principles.
At a high level, these are:

1

Notice

Privacy laws mandate that organizations provide accurate and current notice of their privacy practices.

2

Privacy by design

Privacy laws mandate that organizations think through how their practices may impact privacy rights and the interests of individuals and design their products to comply with those laws.

3

Rights

Privacy laws afford individuals certain rights over their personal data, which may include rights to access, delete, and correct their data.

4

Data minimization

Privacy laws require organizations to practice data minimization (i.e., collect and process only the personal data necessary for the business purposes for which it was collected) and impose retention limits and deletion policies to ensure organizations don't keep what they don't need.

5

Security

Privacy laws mandate certain security standards to protect personal data.

6

Breach notification

Privacy and security laws impose a host of obligations on organizations that experience a security incident or data breach impacting personal data.

 |

The cost of non-compliance

Non-compliance with privacy laws can result in steep penalties, legal fees, and reputational damage. Regulatory penalties under frameworks like the GDPR and CCPA can be substantial enough to materially affect a company's bottom line, while civil litigants may also pursue claims for privacy violations, including class action lawsuits following data breaches.

According to a report from IBM Security and the Ponemon Institute, the average cost of a data breach in 2024 was $4.88 million, which was a 10% increase over the prior year. AON's Cyber Risk Report found that 56 highly publicized cyber events caused 27% share price losses for the impacted organizations on average in 2024. Clearly, this kind of reputational damage can likewise irreversibly impact an organization's competitive advantage. In this landscape, compliance isn't just an expense, it's a strategic investment.

Using Elastic for your data protection compliance needs

Elastic helps organizations find relevant answers that matter at unprecedented speed with open and flexible enterprise solutions. Compliance with privacy laws worldwide requires an understanding of your entire data ecosystem: where personal data resides, how it moves, and how that data is otherwise processed. This is where the Elasticsearch Platform shines, simplifying and automating these processes for seamless compliance. Below, we outline Elastic's value as mapped to the six foundational privacy principles explained above.

Notice

Elastic's data mapping features enable organizations to understand the scope and types of personal data throughout organizational servers and beyond.

Notice is a core foundational principle of privacy laws. Individuals are entitled to understand the types of personal data that an organization collects about them, the purposes of collection, and the circumstances in which their data is disclosed to other parties. Data privacy laws often require organizations to provide comprehensive privacy policies such as Elastic's own Privacy Statement, explaining these concepts as done on the Elastic Trust Center.

To comply with this notice principle, an organization must understand the scope of personal data it collects. This requires a robust data mapping exercise, which is a systematic process that identifies and documents all the personal data flows within an organization.

Without a scalable solution, organizations are often left to rely on a hodgepodge of antiquated spreadsheets, responses to data inventory surveys, and haphazard interviews with various business units to identify personal data collected and how it travels within and beyond the organization.

At best, records may be accurate for a moment in time, only to suffer from the demands of data collection and processing in an economy fueled by data.

Elastic can help organizations gain crucial insights to improve their data mapping processes. Without awareness of the types of personal data collected, where such data is located, and to whom it is disclosed, an organization cannot confirm compliance with privacy laws. By indexing information about your data flows into Elastic, its powerful full-text search capabilities enable rapid identification of applications, tables, queries, or reports that rely on personal data.

Using Elastic to streamline data mapping also helps organizations to comply with contracting obligations of privacy laws, as identified data flows will determine other parties with which an organization should enter into a data protection addendum, data transfer mechanisms, or other agreements specific to the protection of personal data. Likewise, today's supply chains may extend to hundreds or thousands of vendors and subprocessors. The ability to index and perform full-text search instantly through thousands of agreements can also facilitate vendor status reports and, more importantly, enable proactive vendor management programs.

Privacy by design

Organizations can use Elastic to enhance privacy by design, including building in data minimization principles.

If an organization is considering using Elastic as a datastore for personal data, the capabilities of Elastic Cloud Enterprise ("ECE"), Elastic's central orchestration software, can put the organization on the right track from the start. The principle of data protection by design is about treating personal data like a valuable asset by limiting access, maintaining accuracy, implementing appropriate data security controls, and limiting retention periods.

Unlike traditional data architectures with one massive datastore and volumes of complex overlapping data access controls (required for allowing access to only certain data by various projects), Elastic enables users to instantiate new Elasticsearch clusters for each project and include only data relevant to that project in its cluster.

This distributed architecture enables the minimization of personal data — another core privacy principle. For example, customers can use Elastic to categorize data into storage tiers, where access logs information powered by Elastic can help businesses identify unused data to inform data retention policies and practices.

Elastic also enables organizations to understand when and how to conduct data privacy impact assessments ("DPIAs"). Under the GDPR and similar privacy regulations, a DPIA is a sometimes mandatory assessment used to ensure you are processing personal data responsibly and minimizing any potential harm to individuals. Knowing where data lives, how it's processed, and where it flows streamlines completion of DPIAs, which traditionally can require multifunctional support across business units to understand uses of personal data. DPIAs in turn demonstrate foundational compliance while enabling organizations to limit processing of personal data to what is authorized under global privacy laws.

Data subject rights

Organizations can use Elastic to identify relevant personal data, assess applicability of data subject rights, and honor data subject requests.

Global privacy laws give individuals certain choices over how their personal data is processed. These commonly include rights to access, delete, and correct personal data, along with rights to object to certain types of processing of personal data. Elastic's data mapping capabilities form the core foundation by which organizations can process data subject requests.

- **Access:** Elasticsearch allows organizations to search through datastores to identify personal data across the organization, including identifying the tables, queries, reports, or applications that rely on personal data. Organizations can also leverage Elastic to power end user search functions, so that end users can search for their user data. Granting end users powerful search capabilities reduces customer support demands, as end users can use self-serve tools to identify and export their data. Where self-service tools don't suffice, Elastic allows organizations to quickly search their own datastores to honor data subject access requests.

- **Deletion:** After using Elastic to identify the personal data maintained about an individual, an organization can further use Elastic to transform such data, including to tag data for retention under a deletion exception, permanently delete data, and use other deletion techniques that may be permissible under privacy laws, including anonymization and certain types of pseudonymization of personal data. Using Elastic to transform personal data quickly and without costly engineering build helps organizations stay compliant, avoid regulatory scrutiny, and maintain usefulness of data within the limits of global privacy laws.

- **Correction:** Likewise, privacy laws often permit individuals to request correction of their personal data. Elastic can isolate personal data maintained about an individual so the organization can focus on processing the request — not finding the data.

- **Restrictions:** Some privacy laws like the GDPR and its United Kingdom analog also contain a right to object or a right to request restricted processing of personal data. Organizations can use Elastic's data mapping and data categorization capabilities to quickly ascertain how to respond to such requests and restrict access and use permissions accordingly, saving valuable time to enable compliance teams to respond within the short timeframes afforded by these laws.

Data minimization

As previewed in the *Privacy by design* section, Elastic powers data minimization capabilities for enterprise businesses. Data minimization principles mandate that organizations collect, process, and limit retention of personal data to information that is necessary to achieve the organization's authorized purposes of processing.

For example, one way to minimize processing of personal data to meet this obligation is through **pseudonymization** (i.e., replacing personal identifiers in data with placeholder values) or **anonymization** (i.e., fully removing personal identifiers from data so that a person can no longer be identified). Discover how a leading European airline uses the Elastic ingest pipeline to obfuscate sensitive data before storage. Such outcomes can be accomplished using Logstash, an available integration in Elastic that ingests data from a multitude of sources to facilitate transformation of such data — including anonymization and pseudonymization — thereby advancing data minimization goals and reducing data security risks.

Using Elastic for data mapping and auditing also enables organizations to more closely analyze their actual use of retained personal data, allowing the organization to more effectively tailor data retention periods and policies.

Security and breach notification

For more information on how Elastic can help organizations secure their personal data and respond quickly in the event of a data breach, please review our Security White Paper.

Conclusion

Data privacy is not just a regulatory requirement; it's a business imperative. With hefty fines, business disruption, reputational damage, and customer trust on the line, organizations need a reliable, scalable way to map, categorize, manage, transform, analyze, and delete their data. Elastic streamlines every step of this process, providing the scalable power your organization needs for compliance and customer confidence.

