opentext™

5 ways to prepare for data privacy laws

A guide to future-proofing your privacy program

opentext™

Contents

opentext™

Introduction

Since it went into effect in 2018, the General Data Protection Regulation (GDPR) has served as a model for modern data privacy legislation. In recent years, many of the world's most populous countries, and a few US states, have enacted new privacy laws or amended existing laws with similar or overlapping requirements and obligations. As the effective dates of these laws approach and additional privacy laws are enacted, organizations will need to develop a plan to augment existing obligations or address new requirements as they arise.

Building a strong privacy program requires the right combination of skills, expertise, policies, processes, training and technology tools. If a regulation applies to your organization, critical activities are needed to support compliance obligations associated with the processing and handling of personal data. Beyond potential fines, any organizations that fail to comply risk eroding customer trust and damaging their reputation. The to-do list can be long for organizations working to comply with comprehensive data privacy laws. This guide highlights five key initiatives to provide the best "bang for your buck" to help organizations build or improve their privacy programs.

1 Conduct a data processing inventory

An organization cannot comply with data privacy laws unless it knows what personal data it holds, how it is used, where it is kept and what, if anything, has been shared with third parties. Conducting a data processing inventory, also known as a record of processing activities (ROPA), or creating a data map is an important first step.

What to do:

- Identify the relevant departments that process personal data, including HR, finance, legal, procurement, sales and marketing.
- Ask each line of business to identify and document the ways they process personal data. Don't forget data managed by third parties.
- Aggregate the entries and create a centralized master record of all processing activities.
- Document a streamlined and defensible process that can be used to keep the information up to date.

Data processing checklist

For each processing activity it is important to ask the following questions:

- ☑ What type of data is collected?
- ☑ For what purpose is it being collected and used?
- ☑ Does the business have consent to process the data and is it documented?
- ☑ Who is the primary custodian of the data?
- ☑ Who has access to the data?
- ☑ Where is that data being stored and where does it flow?
- ☑ Is there a retention period applied to personal data?
- ☑ Are adequate safeguards in place to protect sensitive data?
- ☑ Is the data being shared with third parties, including vendors?

opentext™

Examples of processing activities include:

- Employee administration
- Employee management
- Recruiting and hiring
- Vendor screening
- Contract management
- Account management
- Customer loyalty programs
- Email marketing campaigns
- Customer event invitations and registration

Having a comprehensive data processing inventory will:

Provide visibility into high-risk areas.

Clarify the link between the data and processing purpose.

Facilitate development of records retention schedules.

Enable better and faster reporting to authorities.

Streamline subject rights requests.

opentext™

Did you know?

In 2020, 64.2 zettabytes of data was created or replicated. By 2025, global data creation is projected to grow to more than 180 zettabytes.[1]

Examples of data categories:

- Customer financial and tax data is retained for the purpose of compliance with tax regulations.
- Newsletter subscribers' information is retained until consent is withdrawn.
- Employee files and records are retained for as long as required by relevant employment laws.
- Direct marketing customer data is retained for a specifically defined period, e.g., two years, unless the customer objects/opts out sooner.
- Customers' contract, service or delivery data is retained for as long as the contract is in force or services/products are provided.

2 Update and implement data retention rules

Gone are the days when organizations could collect as much information about their customers as possible, use that data however they liked and keep it forever. To manage risk, organizations now need to limit retention beyond what is necessary for lawful purposes and ensure disposition activities are in place. This is particularly challenging since the growing volume and complexity of data is making it harder to manage.

Organizations must be able to clearly define:

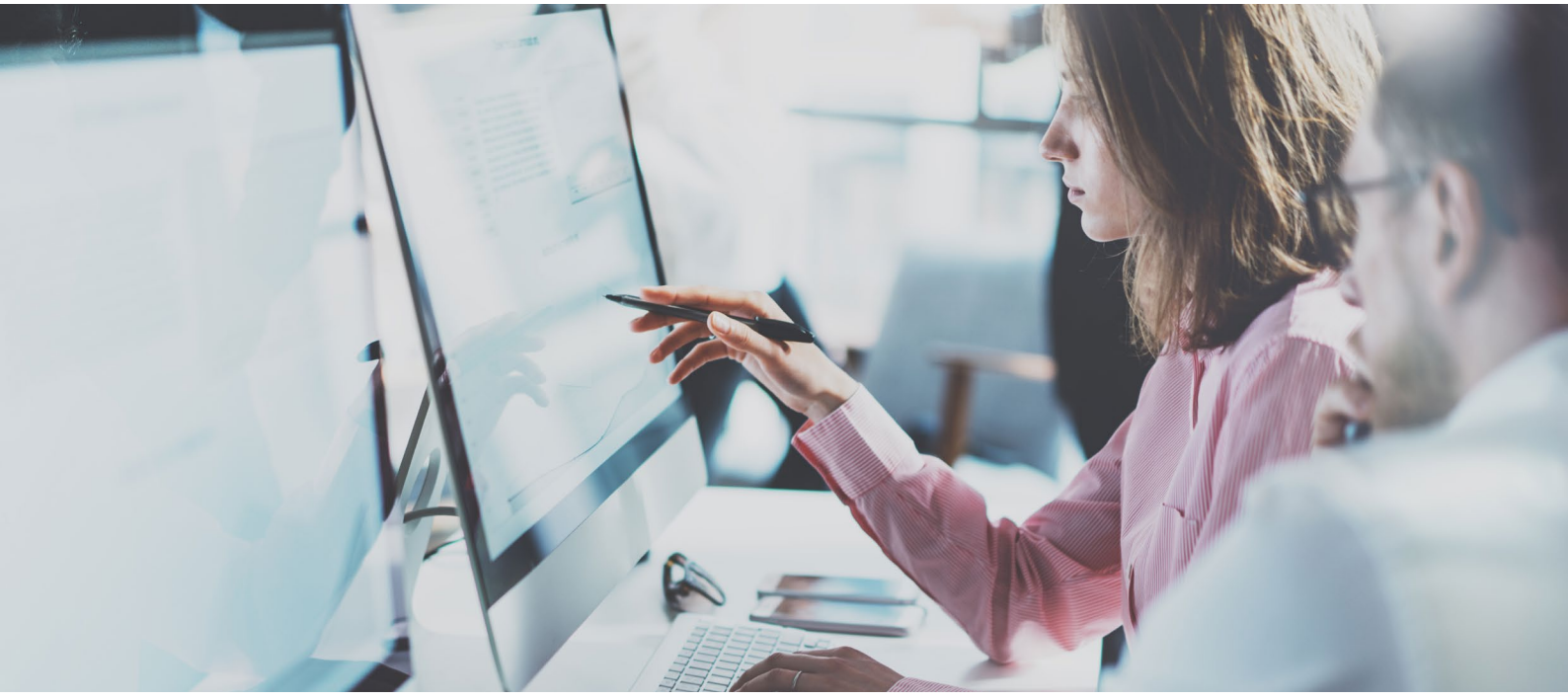
(1) the period for which personal data will be stored, e.g., two years

(2) the criteria to determine that period, e.g., 20 years after a contract has expired, and implement it as policy.

What to do:

- **Start with the data processing inventory**
  Records need to include purposes for processing, categories of personal data and the envisioned time limits for disposition.
- **Find a balance between too general and too detailed**
  Keep it simple. Not every retention period is seven years, but 100 record schedules are probably not necessary.
- **Group data by: (1) type of individual, e.g., job candidates, (2) data categories and (3) relevant purposes**
  It is prudent to relate retention times to such groupings. Establishing and implementing records retention rules is not only a must-have for risk and data minimization, it also makes life easier when it comes to subject rights requests.

1 Statista Research Department, Amount of data created, consumed and stored 2010-2025. (May 23, 2022)



opentext™

Quick tip

One of the best ways to protect personal data is to reduce the risk footprint. Organizations that take an integrated data-centric approach, including for data clean-up activities, will be in the best position to execute on these priorities.

3 Conduct data clean-up

Most organizations store massive volumes of information in ungoverned environments, content repositories, legacy applications and email. Some of that content contains information that can identify individuals and must be evaluated for disposition. Keeping extra personal data can be a liability and expose organizations to regulatory fines and penalties.

What to do:

- Consult the organization's records retention schedules and policy.
- Prioritize high-risk systems that store the most sensitive data.
- Defensibly dispose of personal data:
  - That the organization does not have legal basis to process.
  - Where consent of the individual has been withdrawn.
  - Where consent of the individual has expired.
  - For which approved retention periods have come up.
- Keep audit trails/records of any disposition action taken.
- Leverage tools and analytics to support identification and remediation activities in unmanaged environments.

An integrated data-centric approach to data management

- Locate personal data
- Identify and assess risk
- Understand data usage

- Categorize and classify data
- Establish policy-based retention
- Design and automate processes

- Secure and manage content
- Perform ongoing risk analysis
- Centralize, move and dispose

opentext™

Did you know?

More than half of organizations handle subject rights requests manually, while about 1 in 3 have either partially (32%) or fully (3%) automated the process.[2]

4 Review Subject Rights Requests

Perhaps the most public-facing compliance requirements are the exercisable rights of data subjects/consumers to understand how their personal data is being used. Meeting these requirements is important because non-compliance may result in unhappy customers, statutory penalties and fines. While the scope of these rights may vary, common rights may include, but are not limited to:

- **Right to delete.**
- **Right to correct or rectify.**
- **Right to access.**
- **Right to data portability.**

An organization must develop procedures to respond to these requests, which generally must be performed within a prescribed timeframe, e.g., 30 or 45 days.

Responding to subject rights requests can be time- and effort-intensive, placing a huge operational burden on organizations since there are many steps that must be performed. Even for organizations with mature privacy programs, challenges with information silos, legacy systems and poor search and discovery tools can make it difficult to comply.

For that reason, it is important to establish a step-by-step internal process or checklist that standardizes the handling of subject rights requests.

What to do:

- Complete the data processing inventory.
- Provide an easy way for subjects/consumers to submit requests, such as posting an email address or link on the organization's privacy notice web page.
- Establish a method to verify the identity of the subject/consumer making the request. Are they who they say they are?
- Triage requests to ensure those that are higher risk are addressed first.
- Categorize requests by status, such as new, in progress and completed, and by age. Queue management will be important for meeting strict timelines that may be imposed.
- Identify the owners of major business systems where data is managed, e.g., CRM, HR systems and shared repositories.
- Keep records of requests and their fulfillment or denial as evidence of compliance.
- Track volumes and efficiency to work to continuously improve response time.
- Configure systems to automate the fulfillment process.

2 IAPP, IAPP-EY Annual Privacy Governance Report 2021. (October 2021)

opentext™

Did you know?

76% of consumers felt they were unable to effectively protect their data because it was too hard to understand what companies were doing with their data.[3]

5 Update the privacy notice and privacy policy

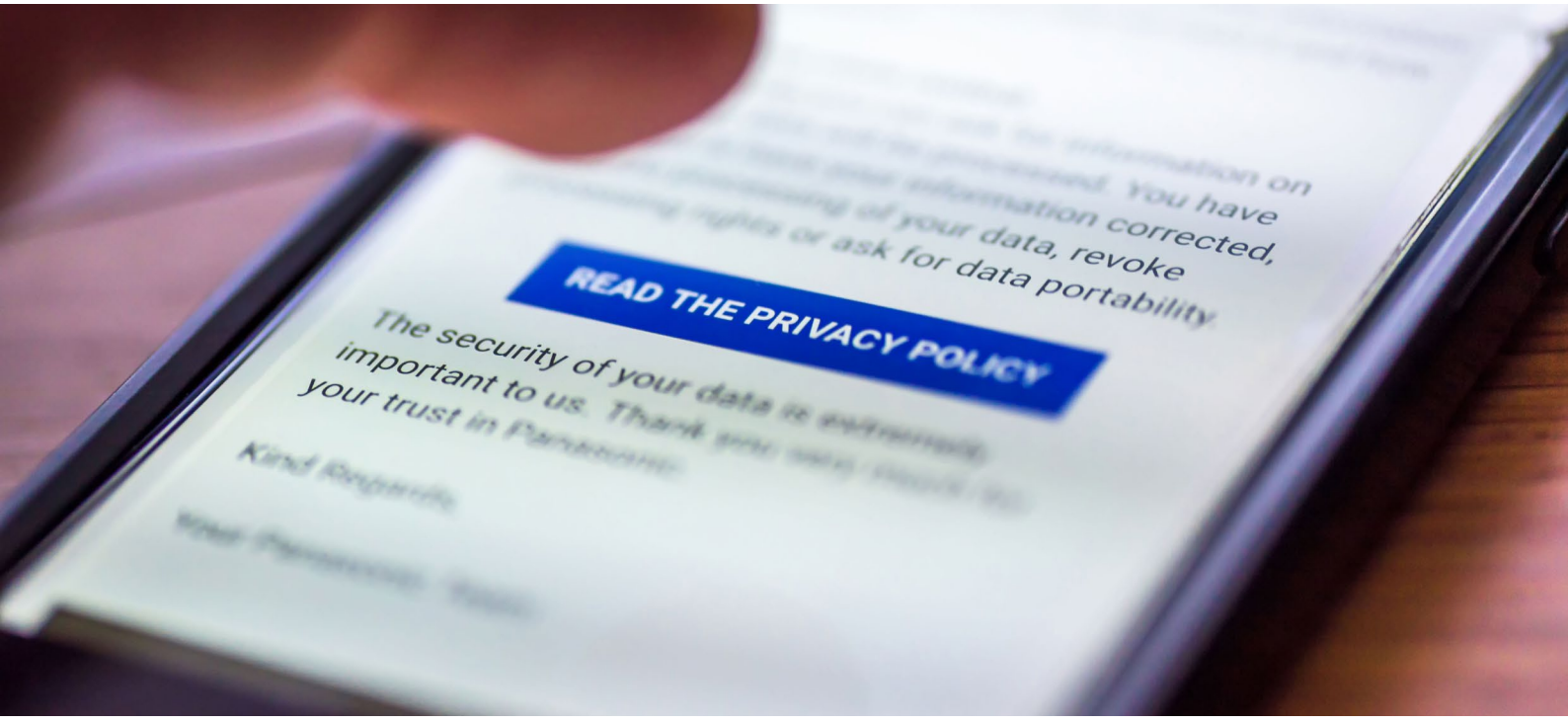
The terms privacy notice and privacy policy are often used interchangeably and, although some organizations combine them, there is a difference.

A **privacy policy** is internally focused, telling employees what they may do with personal data.

A **privacy notice** is externally facing, telling customers and other stakeholders, the categories of personal data processed, the purposes of processing and other specific information required by the law or regulation. It can also be used to disclose how data subjects/consumers can exercise their rights with respect to their personal data.

Organizations should thoroughly review and make additional changes and disclosures to their notices and policies. It is vital that it be written in clear and straightforward language so that explanations are easily understood. This will help reduce concerns or uncertainty regarding how data is being used and facilitate successful implementation of appropriate consent practices for either opt-in or opt-out consent regimes.

3 Cisco, Building Consumer Confidence Through Transparency and Control, Cisco 2021, Consumer Privacy Survey. (2021)



opentext™

Additional resources

- Privacy Management Webpage »
- Solution overview: Privacy Management »
- Blog: The GDPR 4 Years on and beyond »
- Information Governance Webpage »
- eBook: Companies still wrestle with data privacy regulation »
- Brief: Minimizing the Risks with Your Sensitive Data »

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn