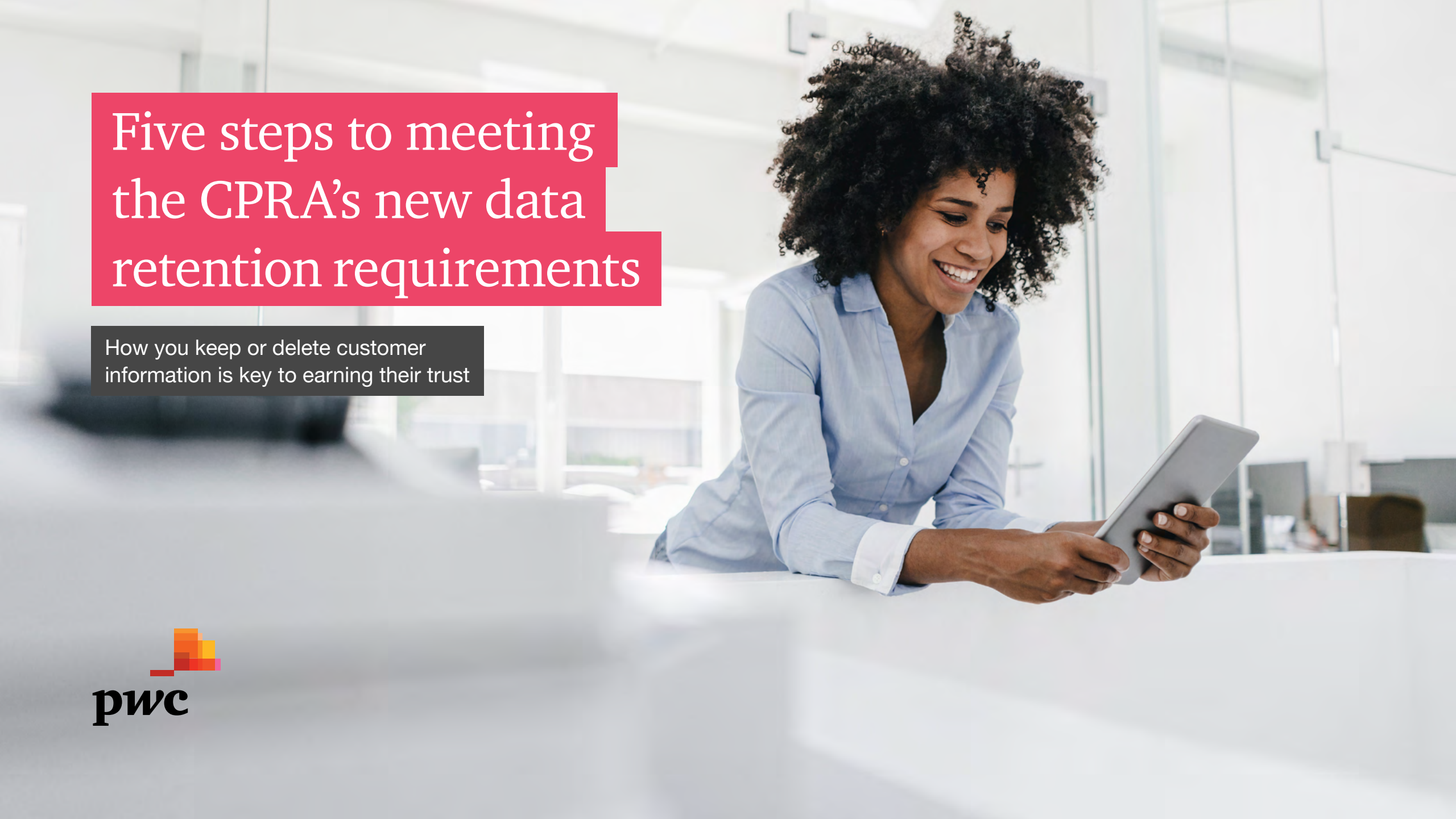
Five steps to meeting the CPRA's new data retention requirements

How you keep or delete customer information is key to earning their trust



pwc

Guide to updating your data retention strategy and program

What most companies have now

Incomplete identification of data	Lengthy retention policies and schedules	Manual and ad-hoc data retention processes	Infrequent or decentralized disposal of data

What they need

Clarity on data assets and retention methods

Next-gen governance of data retention

Investment in the right technologies and tools

Why

Minimize risks, including compliance risks	**Enable sustainable, efficient privacy operations**	**Realize value of data in intelligence and business growth**	**Gain consumer and stakeholder trust**

- Which personal information do you keep on your customers, and how do you decide whether to retain or eliminate it? The wrong strategy can leave your organization vulnerable to privacy intrusions and drive customer and stakeholder mistrust.
- Enter the California Privacy Rights Act (CPRA), a new law prompting new requirements for data retention.
- While CPRA won't take effect until Jan. 1, 2023, companies will need the two years to prepare. Confirm your data and records footprint and review your existing retention capabilities, including technology; right-size, revamp and fully implement your retention policy and schedule; and update required disclosures and agreements.
- Treat the preparations as a time to modernize data retention. Strategically-minded companies will invest heavily in technology to tackle the challenge. They will fold the compliance plan into the overall plan to enhance customer and stakeholder trust.

Why is an effective data retention program more important than ever?

Consumer data trust is falling, not rising. Only 21% of consumers have greater trust in business use of their data, 36% are less comfortable sharing information than they were a year earlier and 85% wish they could trust more companies with their data, according to a 2020 PwC survey.

The California Consumer Privacy Act (CCPA) directly addresses these consumer concerns by requiring companies to disclose which types of personal information they collect, how it is obtained and used, and whether it's sold or shared. The new law, the California Privacy Rights Act (CPRA), which goes into effect Jan. 1, 2023, goes further. It requires companies to disclose how long they keep each category of personal information or, if that's not possible, the criteria they use to determine retention periods.

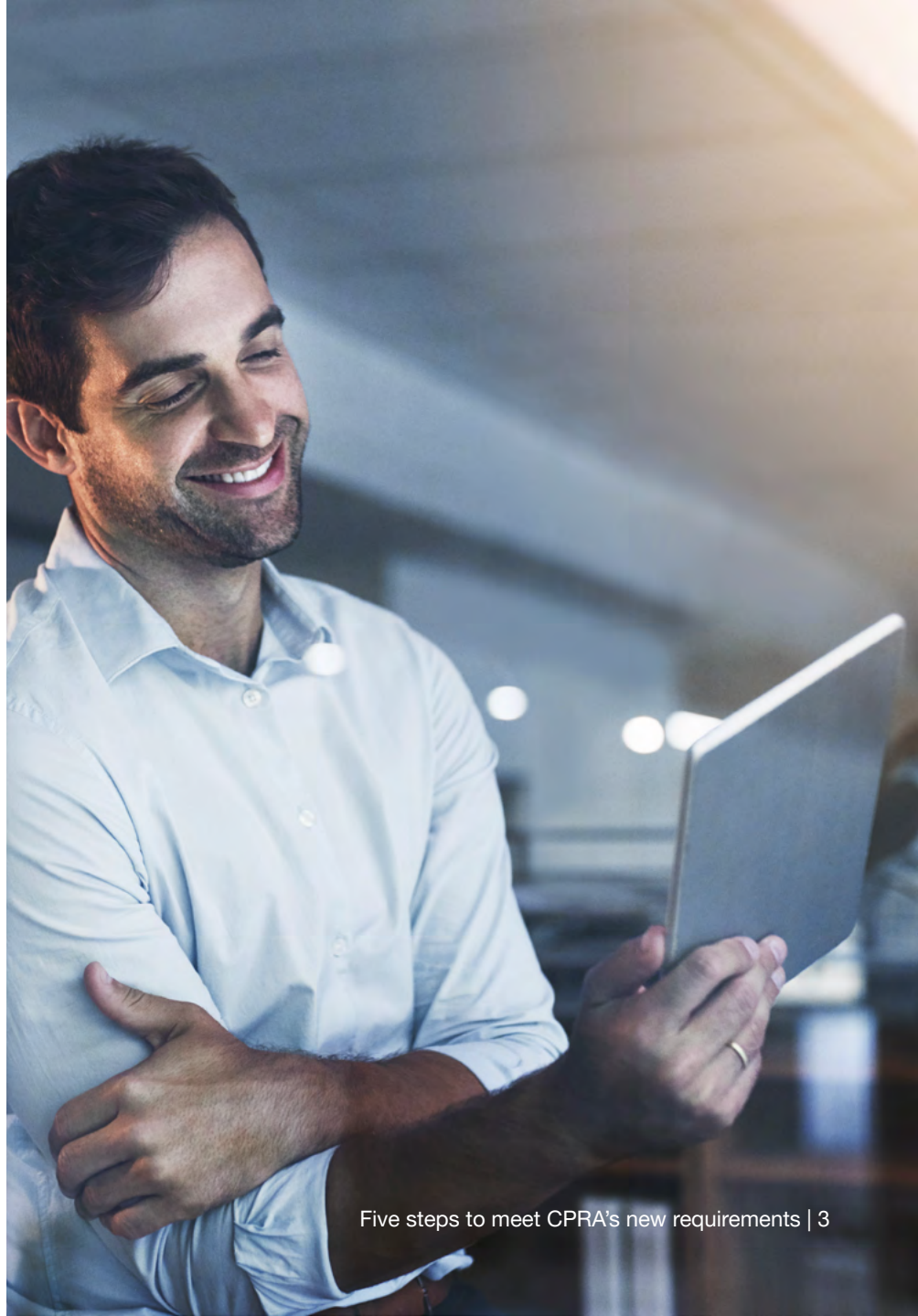
Under CPRA, companies can no longer simply hold on to individuals' personal data forever, at least not without justification and not without notifying consumers, employees and other stakeholders of the decision and rationale for doing so.

The data that's removed is as important, perhaps more important, than the data that's retained. Protecting privacy means collecting only fit-for-purpose data, then keeping and accessing only the data you're required to keep (i.e., the principle of minimization). The less personal information that's retained, the easier it will be for companies to fulfill CPRA-mandated individual requests to access, delete, correct or opt-out of selling or sharing that data. And eliminating obsolete or outdated data will help companies create more accurate and complete personalized experiences for customers.

21%

Only 21% of consumers have greater trust in business use of their data

Source: 2020 PwC survey



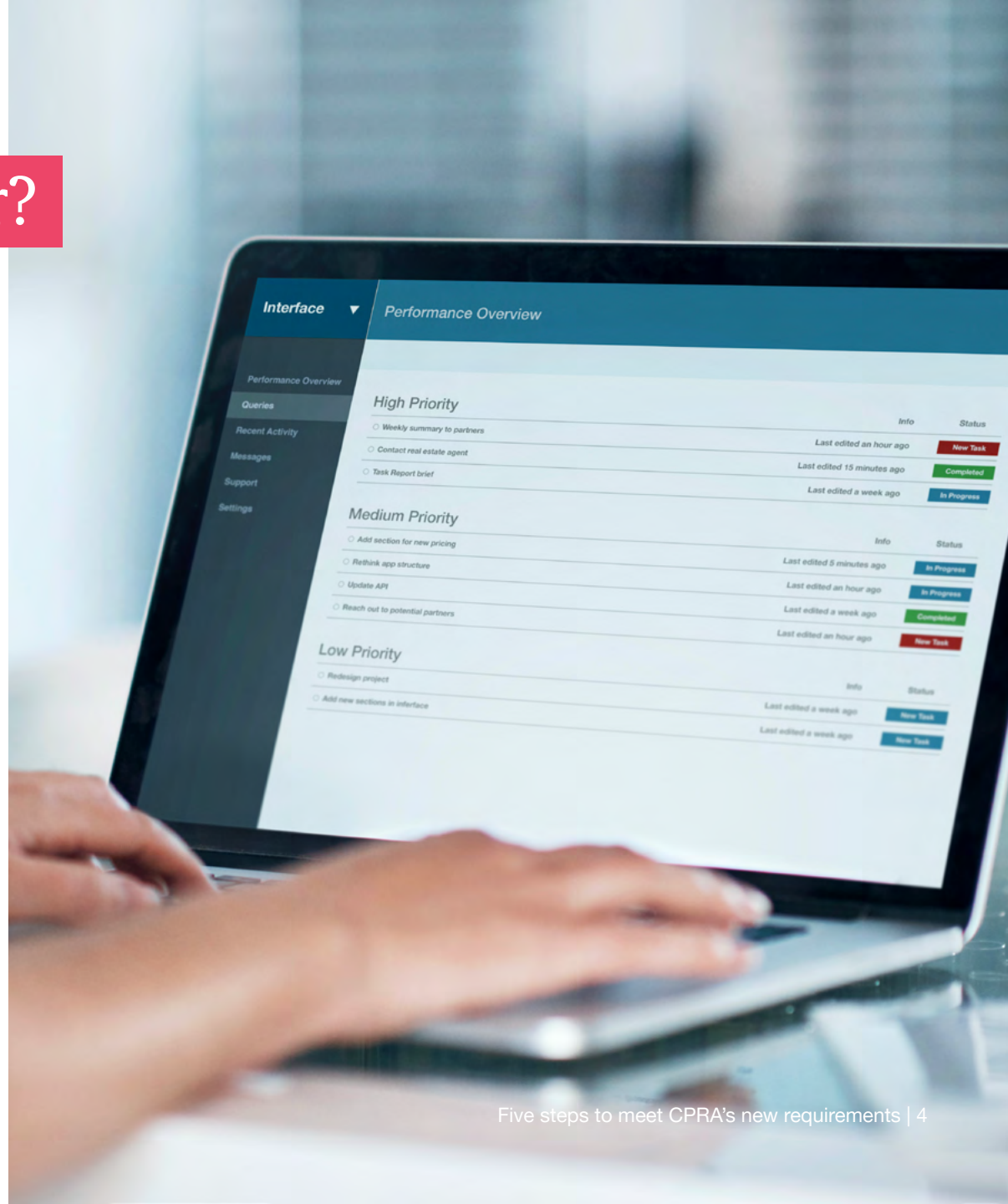
Why is an effective data retention program more important than ever?

More importantly, over-retention of records creates a security and e-discovery risk. In one example, last June, hackers exposed the "BlueLeaks" collection, the term coined for nearly 270 gigabytes of data dating as far back as 24 years taken from hundreds of police agencies across the US. The breach revealed highly sensitive information such as ACH routing numbers and international bank account numbers as well as personally identifiable information and images of suspects — a risk that could have been mitigated if the agencies had effective retention policies in place.

Increasing the cost of noncompliance is CPRA's expanded private right of action, with statutory damages ranging from $100 to $750 per consumer per incident. That's on top of fines from regulatory enforcement actions ranging from $2,500 to $7,500 per violation and the longer-term financial impact resulting from reputational damage and loss of stakeholder trust. What's more, a new California Privacy Protection Agency will have subpoena and audit powers, and it will coordinate investigations with regulators in other jurisdictions, including European data protection authorities.

$100 to $750

Increasing the cost of noncompliance is CPRA's expanded private right of action, with statutory damages ranging from $100 to $750 per consumer per incident.



Will our existing data retention program suffice?

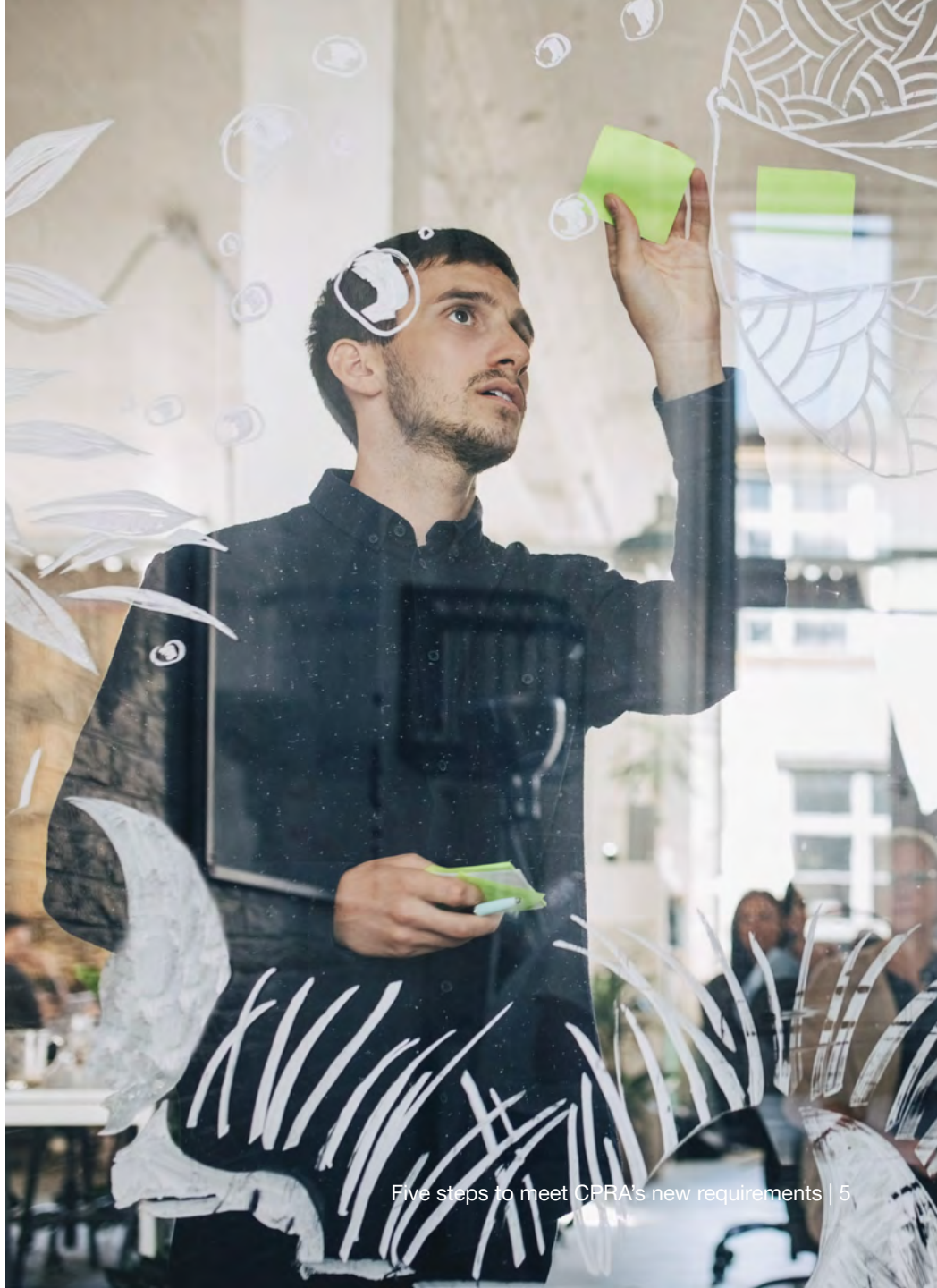
For most companies, bringing retention programs into compliance will be a big lift.

CPRA retention requirements focus on personal information at a granular data category level: for example, personal identifiers along with financial, health, commercial, biometric, geolocation and employment information — personal information that is embedded or referenced in many record types and multiple categories per record. Examples of a customer record include invoices, receipts and targeted mailers. Retention programs have historically focused on these record types, not around the data category level as required by CPRA. That means many companies will probably have to go back to the drawing board on data retention policies.

CPRA requires companies to establish maximum retention periods, not just minimum periods as most of them do now, so they don't hold data indefinitely.

Data under long-term and/or enterprise-wide legal holds need special attention. Current processes for data disposal, once a legal hold is lifted, may be rendered obsolete or invalidated by CPRA.

When should we take action? Now. Most companies will need the two years before CPRA goes into effect to update their data retention programs. Technology may need overhauling or upgrading, and platforms for storing structured and unstructured electronic records may need to be retooled. A roadmap leading to 2023 will be essential.



Five actions you should take immediately

1. Understand and evaluate existing retention schedule, procedures and tools

Which categories of personal information do you collect? What records store this data? How are you managing retention? Use a risk-based and prioritized approach to understand current procedures and tools. Assess your structured and unstructured data as well as automated and manual retention methods. Use the information you gain from the following steps to identify retention risks, policy revisions and operational gaps.

Confirm data and legal scope: Understand the geographic scope of records and data collected and retention-related requirements of applicable privacy laws as you revisit and update your retention schedule. Consider a privacy technology platform to accelerate this effort.

Identify where sensitive and high-priority information categories sit: Use existing data inventories and/or processes, including records of processing activities (ROPAs) and results of privacy impact assessments (PIAs), to identify sensitive and high-priority categories of personal information and support net-new information gathering at scale. For example, you need to know the specific records where a particular category of personal information is stored, whether it's in a structured and/or unstructured format, how long it's held and how it's retained and disposed.

Assess current tools and procedures for executing retention obligations: Confirm your existing tools and related procedures for fulfilling retention obligations for in-scope records, and determine where gaps exist. Where is the company ill-equipped from a people, process and/or technology perspective to dispose of data in line with your retention and disposition policies?

Understand existing non-record disposal policies: Some categories of personal information may not meet the definition of a record. These include extra copies of documents kept for convenience, reference stocks of publications and draft documents that do not contain unique information or that were not circulated for formal approval, comment or action. Review existing policies on the ongoing disposal of non-record information and understand how non-record policies are enforced.

2. Right-size your plan to update your retention policy and schedule

Which data should be kept? How long should it be kept? What do we need to update? Before you overhaul your entire retention schedule, develop a right-sized approach and plan tailored to fit your organization.

Confirm where updates are necessary: Identify the subset of record types that require potential retention period changes, starting with records that include high-risk or sensitive personal information.

Identify and prioritize high-risk record types: Key risk areas within existing retention schedules include where records that contain personal information have been tagged for permanent retention as well as where biometrics and other highly sensitive personal information is being captured and recorded.

Determine updates to retention periods: Legal, privacy, data and information governance teams should determine appropriate retention periods at a record and data category level. The business, which ultimately determines use cases for data, is also integral to this process, particularly when it comes to setting and justifying minimum and maximum retention periods.

These teams should consider legal retention requirements and use cases, privacy-related exceptions (e.g., for CPRA) and rules of agencies such as the IRS, HIPAA and OSHA. Legal retention requirements can be used as the baseline for determining retention periods.

The retention period can be a set time frame — three years after an account is no longer active or after contracts or relationships are terminated, for instance.

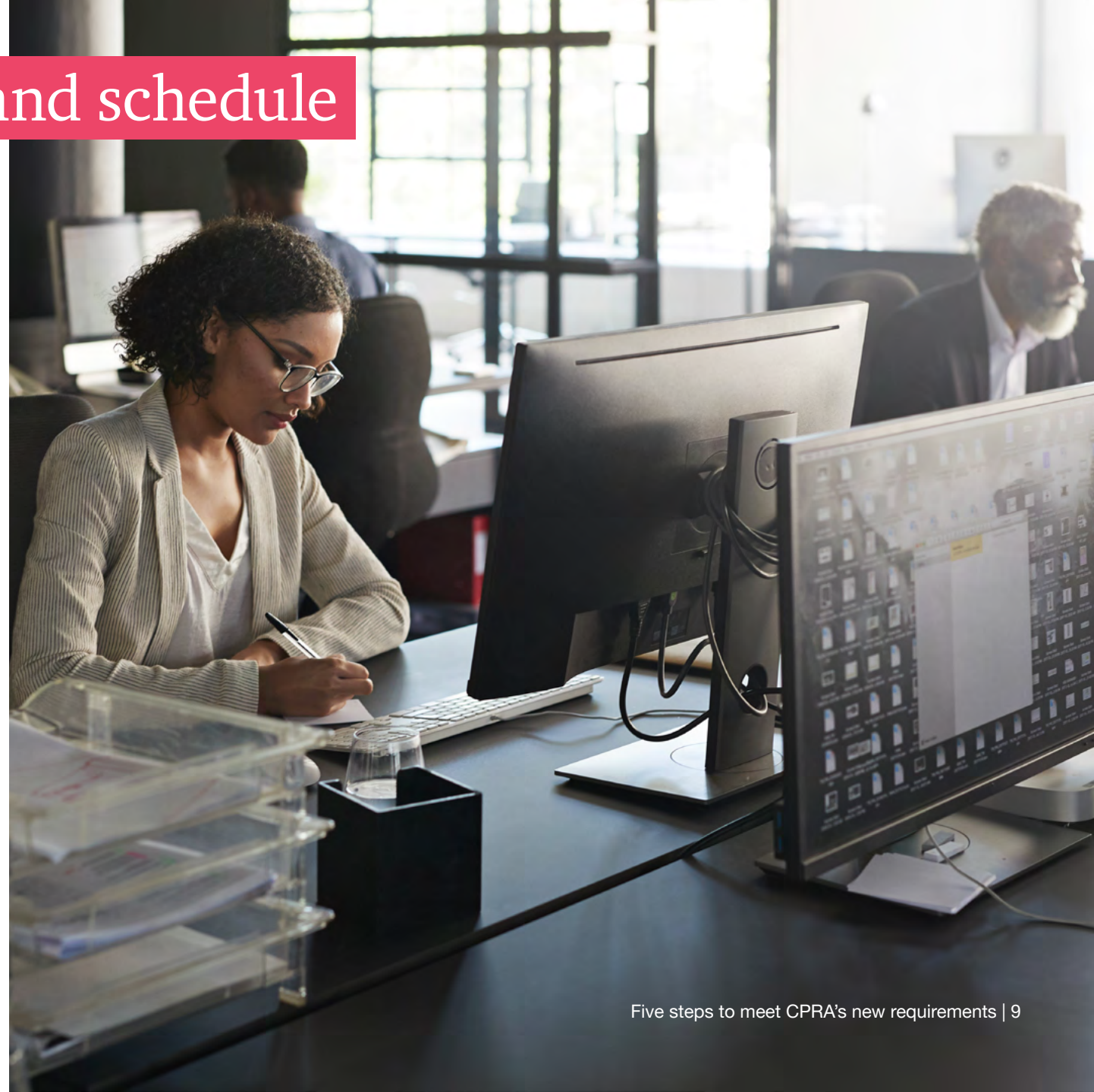
Determine go-forward mechanisms for disposal: Deletion may not always be the right disposal approach. In some cases, it could mean de-identification, which can be helpful in balancing long-term analytics needs. Determine how you'll dispose of each record type containing personal information in both structured and unstructured formats.

3. Revamp retention policy and schedule

You've identified and prioritized relevant categories of personal information, record types and needed updates to retention periods. Now it's time to update your retention policy and schedule.

Record retention schedules typically follow a "big bucket" approach, grouping retention requirements into large buckets to reduce and streamline operational complexity. CPRA dictates that you adjust those schedules to account for additional granularity and for non-record disposal.

As the schedule is updated to incorporate these new privacy requirements, continue to look for opportunities to streamline operations. Minimize the number of records for permanent retention and limit the number of "event trigger" requirements to minimize operational overhead.



4. Fully implement the retention schedule, including supporting technology

Engage with business stakeholders to appropriately map the revised retention requirements to the data and information assets in your organization. Plan for change management so that enforcing the updated retention policy doesn't negatively affect your business.

Implement routine disposal processes: Particularly when it comes to personal information, a trigger depends on when the data is no longer needed. Evaluate and implement triggers in new or existing business processes to identify and dispose of this data in a timely manner in accordance with your updated retention schedule. Incorporate exception processes to address legal holds or other regulations, including anti-money laundering and Know Your Customer requirements.

Implement incremental technologies and tools: Retention management tools and other new technology can help automate timely disposal of data. You can use third parties to host and manage retention of data on your behalf, but this approach carries risks. Your company will need specific contractual provisions and monitoring capabilities to ensure the third party's adherence to retention requirements.

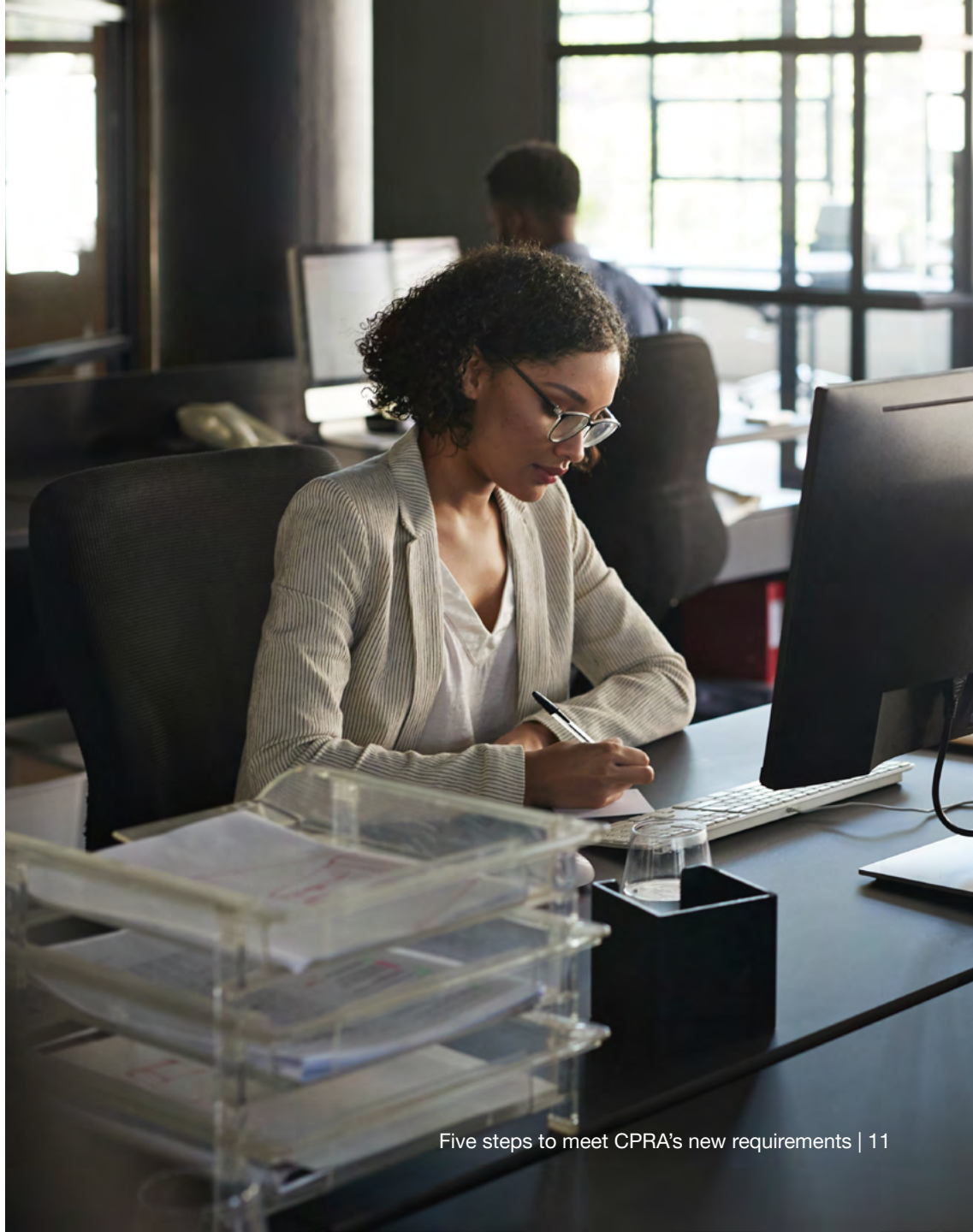
5. Update required disclosures and agreements

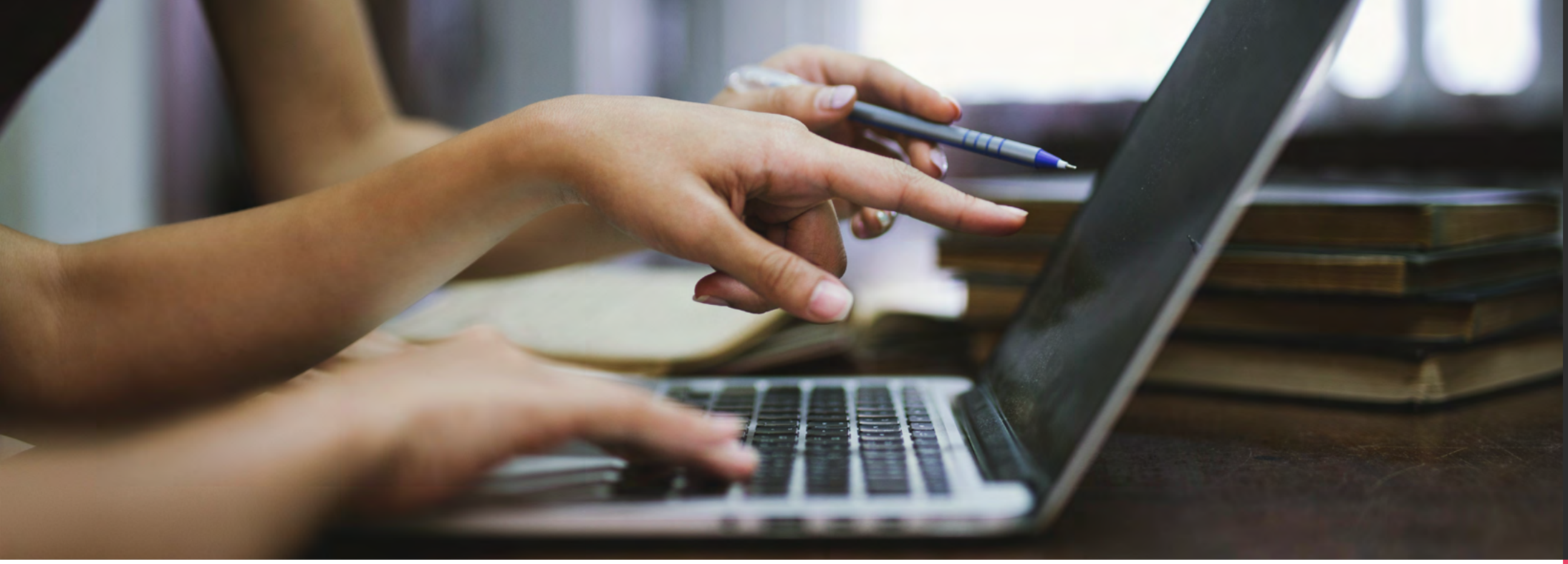
Customers need to know how you're better protecting their data through enhanced data retention policies. Update your privacy notices to reflect required disclosures around retention of personal information.

Determine approach to disclosures: The level of detail can vary. One organization might disclose the actual retention periods for each category of personal information, while another might simply disclose its method for determining retention periods, an alternative provided in CPRA.

Consider stakeholder privacy experience: When updating your privacy notice, consider what experience you want for your customers. Include information about your organization's privacy stance and privacy platform, consumer navigation of privacy features, and how you handle data. The notice language should be easy for consumers to understand. Also review existing third-party contracts and amend them to include sufficient provisions for retention requirements.

Our PwC colleagues Joe DeMarzio and Neha Thakrar contributed to this article.





Contact us

How to help bring workers onsite safely, manage risk and build their confidence

Joshua Rattan
Principal, PwC US

Jay Cline
US Privacy Leader, Principal, PwC US

Joseph Nocera
Cyber & Privacy Innovation Institute Leader, PwC US

Sean Joyce
Global Cybersecurity & Privacy Leader, US
Cyber, Risk & Regulatory Leader, PwC US

© 2021 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This document is not intended to provide legal or medical advice. Please consult with legal counsel and medical professionals as part of your return to work protocols as appropriate. 1082980-2022