



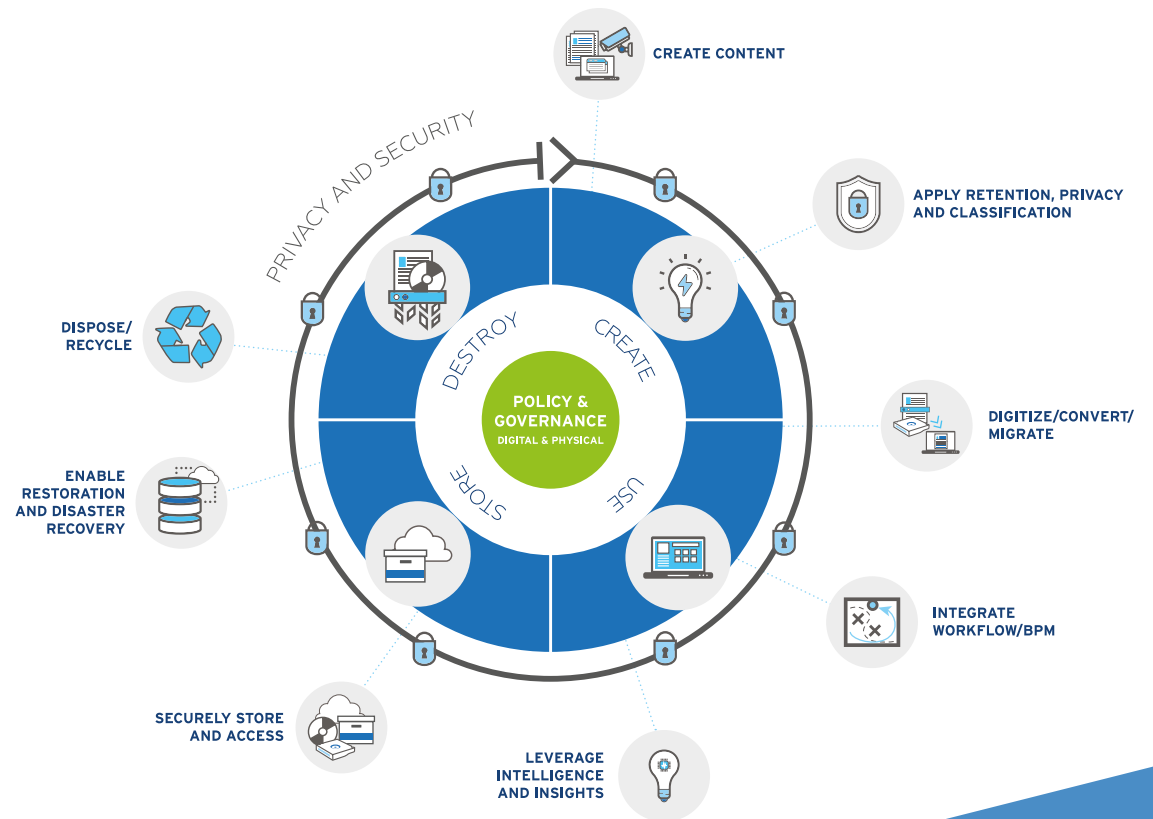
PRIORITIZING CCPA PRIVACY

INTRODUCTION








The California Consumer Privacy Act (CCPA) was enacted on January 1, 2020 as a response to increasing consumer privacy concerns. The CCPA influences how states protect consumer's personal information and allows California residents to request to see all information a company has saved on them, as well as a list of third parties that a company may have shared their data with. No matter how experienced an organization may be, compliance right now is a daunting task.


How can organizations ensure their privacy program complies with the CCPA requirements? The key to a successful privacy program is to manage your information throughout its lifecycle with strong governance rooted in policy. Privacy is a part of virtually every component in the information lifecycle, from the creation or receipt of data, to using it within workflows or for analysis, and ultimately determining appropriate storage and disposal requirements. A strong information lifecycle management program protects your organization from risks associated with compliance and is vital to protecting customer privacy and business success.

No matter which privacy law, you're looking to adhere to, a strong information & data foundation will help you comply with the law and make the most of your data. As you read through this eBook, you'll find expert advice, organized into key chapters, that illustrates the path of a successful information lifecycle management program from beginning to end.



CONTENTS

 UNDERSTANDING THE IMPORTANCE OF ILM	4
 MANAGING YOUR ORGANIZATION'S PERSONAL DATA	6
 DATA MIGRATION FOR 'OFFLINE' RECORDS	8
 MANAGING DATA RETENTION AND PRIVACY TOGETHER	10
 REVISIT YOUR DATA BACKUP STRATEGY	12
 DISPOSAL OF PERSONAL DATA	13
 KEY TAKEAWAYS	15



UNDERSTANDING THE IMPORTANCE OF ILM

As the clock ticks toward the Jan. 1, 2020 effective date of the California Consumer Privacy Act (CCPA), the regulated community rushes to understand the proposed regulations that will implement it. No matter how experienced an entity happens to be, compliance right now is a daunting task. So where should an organization begin? With a successful information lifecycle management process in place.

As each day brings affected businesses ever closer to the deadline for complying with the new CCPA law, those outfits must also work through the layered data protection requirements of other jurisdictions that have already delved into this area. Even more requirements being developed by other nations and states are on the horizon. A sensible approach to this dizzying array of requirements involve managing your information throughout its lifecycle with strong governance rooted in policy. Without a strong information lifecycle management program, it's just not possible to ensure compliance and effectively protect, valuable, sensitive information.

WHY IS DATA PRIVACY COMPLIANCE SO COMPLICATED?

Organizations with even the best intentions regarding their customers' data privacy are challenged to adhere to increasingly complex data protection requirements. The precise laws and regulations any given organization must comply with can depend on a host of factors, like how large it is, where its customers and users are physically located, and the type of data it handles.

Deadlines for compliance vary, too. Although the CCPA becomes effective on the first of the New Year, its requirements will not apply to business-to-business communications and employee information, or to the information of prospective hires, for another year.

The material covered in the various requirements has differing definitions, as well. Some laws, like the CCPA, govern personal information. What exactly is considered personal information or personal data can vary, though, depending on how a specific jurisdiction defines it. In sum, determining exactly how to comply with such a complex web of privacy requirements can be an overwhelming task.



HOW CAN AN INFORMATION LIFECYCLE MANAGEMENT PROCESS HELP?

Information has its own circle of life within an organization – it will be planned for, created, used, stored and eventually disposed. An organization's stakeholders will have different roles in shepherding that information, with the possibility of some overlap or an ineffective siloing of roles (for instance, with IT, records and information management teams working separately). Separate policies and procedures might apply to different stages of a piece of information's existence, so there could be even more overlap. Other stakeholders, such as lawyers and privacy teams, are also likely to voice an interest in what is happening.

An information lifecycle management process can help organizations get a handle on all of these moving parts, varying interests and roles, and, most importantly, obligations. In a moment of rapid regulatory change, records retention and data privacy policies and procedures need to be connected, updated and compliant with varying requirements.

BUSINESSES AND INDIVIDUALS WILL SPEND \$467 MILLION TO \$16.45 BILLION TO COMPLY WITH REGULATIONS IMPLEMENTING THE CALIFORNIA CONSUMER PRIVACY ACT.

SOURCE: ECONOMIC IMPACT STATEMENT FROM THE CALIFORNIA ATTORNEY GENERAL

WHERE TO FIND INFORMATION LIFECYCLE MANAGEMENT EXPERTISE

Admittedly, many working in the data management field are trying to become privacy experts quickly, as their organizations hustle to comply with various emerging requirements. But with such a valuable asset, it makes sense to get outside help from experts that have made information management their constant mission.

Iron Mountain's Information Governance Advisory Services will work with you to implement an information lifecycle management program to help with your privacy program. Their expert team can also support organizations as they develop or improve their processes to handle requests from individuals exercising their rights under the CCPA and other laws.

Stay current with requirements by using the Iron Mountain cloud-based Policy Center Solution Enterprise Edition, which is supported by the Advisory Service team. High-quality research from Iron Mountain's international network of law firms lets organizations know how changes impact them. You'll be able to create visual maps to centrally see where personal data lives, who owns it, what process it's a part of and what are your retention rules and privacy obligations for it. Policy Center is integrated with Iron Mountain InSight® and Workflow Automation™ powered by Hyland.

Fast-paced changes have made for an exciting and sometimes overwhelming moment in the information management world. Be prepared by putting an effective information lifecycle management process into place.

MANAGING YOUR ORGANIZATION'S PERSONAL DATA

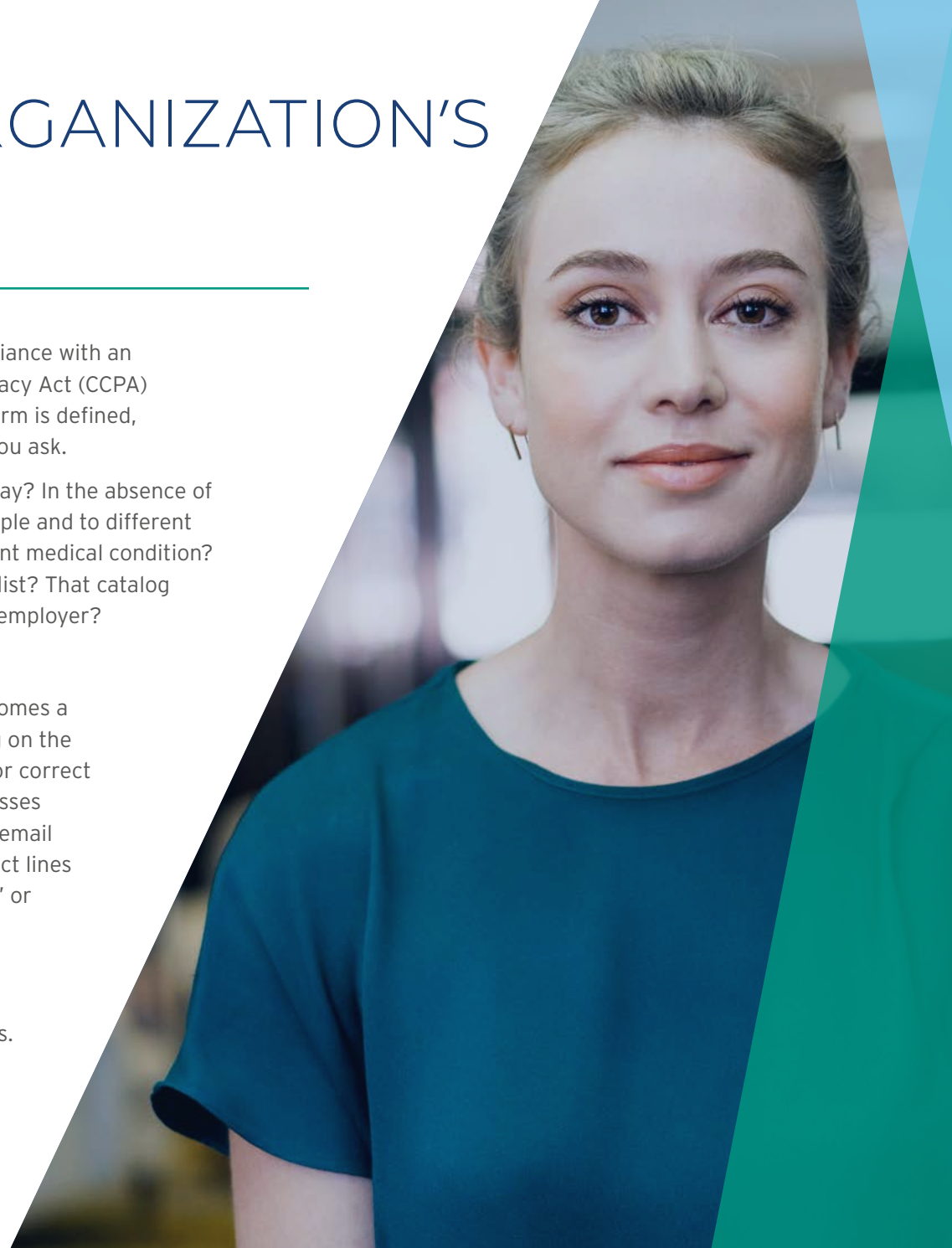
For an organization to manage personal data responsibly – and in compliance with an increasing array of laws that govern it, like the California Consumer Privacy Act (CCPA) – it needs to know exactly what so-called “personal data” is. How that term is defined, and which privacy laws affect your organization, can depend on whom you ask.

Have you defined personal data for your organization in some specific way? In the absence of a global definition, the phrase can mean different things to different people and to different regulators. Does it include your name? Your fingerprint? Your most recent medical condition? Your cell phone number? Your voter registration status? A product wishlist? That catalog of accomplishments you included in a cover letter sent to a prospective employer?

WHY DOES DENOTATION MATTER?

Simply defining what personal data actually is for your organization becomes a more complicated task when the implications are considered. Depending on the jurisdictions they live in, customers and users have varied rights to see or correct their private data or to have it deleted entirely. Even the smallest businesses tend to have personal data of some sort, even if that just happens to be email addresses and credit card numbers. Larger operations with varied product lines or services will have collected more data of all kinds, whether “personal” or not. To comply with laws like the CCPA that cover personal information, an enterprise needs to determine what data it has, where it is handled and stored, to whom the data belongs and the data owner's rights.

Remember, too, that data privacy laws do not just apply to digital records.



THE INITIAL COST FOR A TYPICAL BUSINESS TO COMPLY WITH THE REGULATIONS THAT IMPLEMENT THE CALIFORNIA CONSUMER PRIVACY ACT IS \$75,000.

SOURCE: ECONOMIC IMPACT STATEMENT FROM THE CALIFORNIA ATTORNEY GENERAL

CLASSIFYING PERSONAL DATA FOR YOUR ORGANIZATION

To comply with data protection requirements, an organization needs to define personal data and then figure out where it is. Because laws and regulations covering personal data are varied and complex all on their own, you may want to get some assistance with classifying personal data for your organization. Even if an enterprise already has defined personal data, that operating definition may need to be updated and revised to reflect recent legislation and other requirements.

The Iron Mountain Information Governance Advisory Services team, staffed by experts who understand this quickly evolving field well, can help enterprises on their compliance journey. Determining exactly what personal data is and then locating all of it is not a simple or quick task. Having an experienced team yields greater efficiency. Given the potentially devastating consequences of mishandling personal data – regulatory fines, bad public relations and loss of customer goodwill – choosing the right help becomes even more important.

FIGURE OUT WHERE ALL THAT PERSONAL DATA IS

After defining personal data for your organization, determine where all of that data lives so that it can be protected and managed appropriately in compliance with current requirements. To that end, an organization may need to launch a project to identify legacy records containing personal data. That information may not just be in the cloud, but also on actual paper, tapes or even microfiche.

Consider getting some content classification help

so that you will know what needs to be retained pursuant to current legal requirements and what can be discarded. This exercise can also enhance accessibility, which may become increasingly important as consumers exercise their rights to know what information an organization has collected about them and opt to have it corrected or deleted.

It's a daunting task, but it doesn't have to be – the Iron Mountain Content Classification Service can help businesses address a sometime confusing litany of retention requirements. Relying on an experienced service provider can also boost an organization's confidence should it be subject to an audit, enforcement action or a lawsuit.

NEXT UP: MAPPING AND MANAGING PERSONAL DATA FOR YOUR ORGANIZATION

Classifying data will not be a “one and done” effort. To make the classification useful, develop a data flow map that shows where personal data resides and how it is shared and/or moved between applications and repositories. This is mandatory for some privacy laws and helps identify sources of breached data. With Policy Center, you'll be able to create visual maps to centrally see where personal data lives, who owns it, what process it's a part of and what your retention rules and privacy obligations are. These data flow maps enable quick access to documents with personal data to comply with privacy laws, such as “right to be forgotten”.

Advanced technologies analyze your structured and unstructured data and can give insight into where personally identifiable information (PII) is located. Iron Mountain InSight® reduces risk by using machine-learning based classification to identify and tag PII.

DATA MIGRATION FOR 'OFFLINE' RECORDS

With all of the talk about complying with the California Consumer Privacy Act (CCPA), extending its protections to an entire customer base and adhering to similar laws around the globe, it can be easy to hyper focus on digital data. Yet, if data migration is not top-of-mind in all of these efforts, it should be.

Currently, organizations are rushing to update their online privacy notices to meet California's requirements and conduct data-mapping exercises, so that when consumers ask about their data, these enterprises will be able to find it. What businesses need to remember as they work on these tasks is that not all of their records containing personal information are in an electronic format. To that end, data migration – converting paper and other records to searchable, retrievable ones – might need to be on a CCPA to-do list.

DATA ISN'T JUST DIGITAL

California's law specifically mentions non-digitized records: "The provisions of this title 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," reads Section 1798.175 of the statute. In case that verbiage isn't convincing, consider California's proposed regulations implementing the law. The proposed rules address the "offline" practices of businesses more than a handful of times.

For some entities, accessing "offline" information is likely to be a challenge. After all, consumers' personal information might be on paper records – it might be organized (as in, neatly filed in a cabinet or box at a distant location), or it may not be. Enterprises that have been in business for a while might have stored legacy records using technologies current for their time, like microfiche and tapes. Searching for keywords in these offline materials would be time-consuming, so if there was ever a good moment to transition these materials to a digital format, now would be ideal.





THE U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION HAS MORE THAN 5 MILLION CUBIC FEET OF ARCHIVAL RECORDS. THAT IS THE EQUIVALENT OF 12.5 BILLION PAGES.

SOURCE: DELIVERING GOVERNMENT SOLUTIONS IN THE 21ST CENTURY

WHEN TO BEGIN DATA MIGRATION

Many businesses have been meaning to get around to this sort of thing, but haven't felt the need to make it a priority. They might not have as much archived material as the U.S. National Archives, but they probably have some. The imminent January 2020 effective date of the CCPA may incentivize organizations to inaugurate data migration projects for any offline information sitting in their archives.

As organizations perform compliance activities to adhere to California's requirements and anticipate data privacy regulations in other jurisdictions, a logical way to deal with offline materials is by scanning paper documents, determining whether they contain personal data, tagging them for searches, and then deciding if they need to be retained or securely destroyed.

Part of the project may include transitioning data from older formats (remember video tape?) to newer ones for an assessment – all personal information should be identified, tagged for searchability, and then evaluated for retention or appropriate destruction.

HOW TO GET DATA MIGRATION HELP

As enterprises strive to comply with various data protection requirements, they must simultaneously continue to fulfill their organizations' missions. It makes sense for an organization to focus on growing its business while getting outside help to manage "offline" data from a service provider that has made a career of doing just that.

Iron Mountain's InSight® Essential Edition is a subscription solution that combines Document Scanning of physical documents and digital storage in a secure cloud repository. Leveraging Iron Mountain Document Scanning experts, equipment and cloud storage platform, you'll be able to centrally access your information, free up valuable workspace and make handling of your information and its usage much easier.

For organizations that need to move data from microfiche, tape or other formats, Iron Mountain offers Data Restoration and Migration services to make the transition easy with useful, searchable results.

Once records have been digitized, Iron Mountain's Secure Shredding services can safely dispose the paper versions in a compliant, safe and cost-effective way.

MANAGING DATA RETENTION AND PRIVACY TOGETHER

As organizations focus on compliance with the California Consumer Privacy Act (CCPA), they may realize that managing privacy and data retention go hand in hand. Cradle-to-grave management of personal information from its creation to its responsible disposition can help minimize the generation of unnecessary personal information in the first place and help ensure its proper handling, retention and disposal.

Companies on their CCPA compliance journey might pause for a moment on data retention. “We’ve already dealt with that,” some might say, pointing to their organization’s longstanding data retention policy. But when was that policy promulgated or last updated? Was it drafted in a silo of sorts in days before the term “personal information” became commonly used? Has anyone looked at that policy recently to see if it does address retention of any sensitive information beyond, perhaps, confidential business information? And, in all honesty, how well is the policy actually being followed?

BEWARE DATA HOARDERS

There can, for instance, be a tendency to keep emails forever. Or, at the very least, for far longer than they need to be. A recent report found that 62% of organizations struggle against a “keep-everything” culture. In the real world, those bits of correspondence can be a professional lifeline for an individual user: They typically are easily searched and retrieved and can help reconstruct agreements, serve as reminders of to-do lists, and aid immeasurably in fostering good business relationships.

At the same time, emails at the office may well contain what now is deemed to be personal information subject to California’s privacy law and possibly a host of others as well. Emails tend to be “unstructured” records that are not in a formal database or file structure.

Those emails are not alone in that “unstructured” category. All sorts of data can be unstructured – such as images or videos, social media posts or word processing documents.

ON AVERAGE, 90% OF DATA THAT IS GENERATED DAILY IS UNSTRUCTURED.

SOURCE: FORBES, "WHAT IS UNSTRUCTURED DATA AND WHY IS IT SO IMPORTANT TO BUSINESSES? AN EASY EXPLANATION FOR ANYONE", OCTOBER 16, 2019.

WHY THE CONCERN?

Any number of organizations certainly have been able to function without, perhaps, giving a whole lot of thought to whether their data is structured or not. Now, however, with consumers more interested in learning what private information an organization may have about them, and with legislators providing them the means to obtain it, structured data has taken on greater importance. Why? Because it is easily searchable.

With increased focus on personal information and the need to release it, upon request, to the very people addressed by it, more care – and management – needs to be given to the maintenance of privacy and retention from the get-go. Privacy and retention should no longer be handled in separate silos.

Traditionally organizations have the Records & Information Management department govern policy for how long to keep records and then, separately, have a privacy team manage the privacy policy for records. Managing privacy, retention and your information together throughout its lifecycle is crucial to maintaining compliance and protecting valuable information. This integrated approach allows organizations to:

- › Have a unified view of personal data and related obligations
- › Dispose of private information as soon as possible
- › Reduce unnecessary exposure to data breaches.

The goal, of course, is to minimize generation and retention of personal information by limiting it to that which is necessary to conduct an enterprise's mission. Rather than retain quite so much, today's emphasis is on reducing and, as appropriate, disposing of it in an appropriate way. The failure to do so opens an organization up to not only the risk of a data breach, but also the risk of being found non-compliant with applicable regulations and facing potential reputation-ruining consequences.

WHERE TO GET HELP

Handling privacy and data retention together can be a daunting task, particularly where unstructured records are involved. Organizations can leverage the ML and AI functionality of Iron Mountain InSight® to automatically classify, extract and enrich physical and digital content.

As information moves through business workflows, organizations need an easy way to identify retention requirements. Iron Mountain's Advisory Services team can help customize an organization's document retention rules. By leveraging Iron Mountain's Policy Center solution – which is now integrated with Iron Mountain InSight® and Workflow Automation™ powered by Hyland solutions – organizations can also automate document retention and improve compliance.

As enterprises strive to minimize their privacy risks, turning to outside expertise can help as they continue on their ever-changing compliance journey.

REVISIT YOUR DATA BACKUP STRATEGY

An organization typically develops a data backup strategy as a means of ensuring business continuity when disaster strikes. But, businesses subject to the California Consumer Privacy Act may need to revisit their data protection backup strategies so that personal information is not inappropriately stored, or restored.

Have you given any thought to your data backup strategy in light of the California Consumer Privacy Act (CCPA)? Data must still be backed up, of course, but an organization's strategy for doing so may need to be tweaked for compliance with the CCPA and other data privacy laws.

Enterprises back up data so they can rebuild after a catastrophe, such as a hurricane, destructive hack, infection by ransomware or some other calamity. A data backup strategy remains a vital element of disaster preparedness that goes a long way toward recovery should an unfortunate event take place.

BACKED-UP DATA SUBJECT TO THE CCPA

Organizations subject to California's privacy law must delete the personal information of a consumer upon request. Backed-up data gets a slight reprieve, but is still covered by the law.

California's proposed regulations implementing the law explain that "if a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used."

Businesses subject to the CCPA's requirements need to put a plan in place to handle CCPA deletions of private information in backup data.

REVISIT PERTINENT POLICIES AND PROCEDURES

Backed-up data could be stored on dozens of tapes in multiple locations, so a consumer's personal data might not be easily searchable. An organization may not even be certain which tapes contain what sorts of personal data.

Data backup strategies can be addressed in records retention policies and procedures, which may need an update in light of California's consumer privacy requirements. Data backup strategies might also be mentioned in information security policies or data privacy policies.

Data-mapping exercises may need to be conducted for backed-up data. Organizations need to know where personal information in backed-up data is, so they can delete it upon a consumer's request.

How might a data backup strategy change? Removing a consumer's personal information from backed-up data may mean that organizations need to conduct backups more often. That way, they won't recover data from a point prior to the deletion.

It is also possible that consumers will be so reassured by the precautions taken by organizations subject to California's privacy law, that they actually become willing to provide more personal information in order to make their consumer experience better. In that scenario, it is possible that businesses subject to the CCPA may actually need to increase their backup storage.

THE VALUE OF CONSUMERS' PERSONAL INFORMATION PROTECTED BY THE CCPA IS ESTIMATED TO BE \$169 MILLION.

SOURCE: STANDARDIZED REGULATORY IMPACT ASSESSMENT: CALIFORNIA CONSUMER PRIVACY ACT OF 2018 REGULATIONS

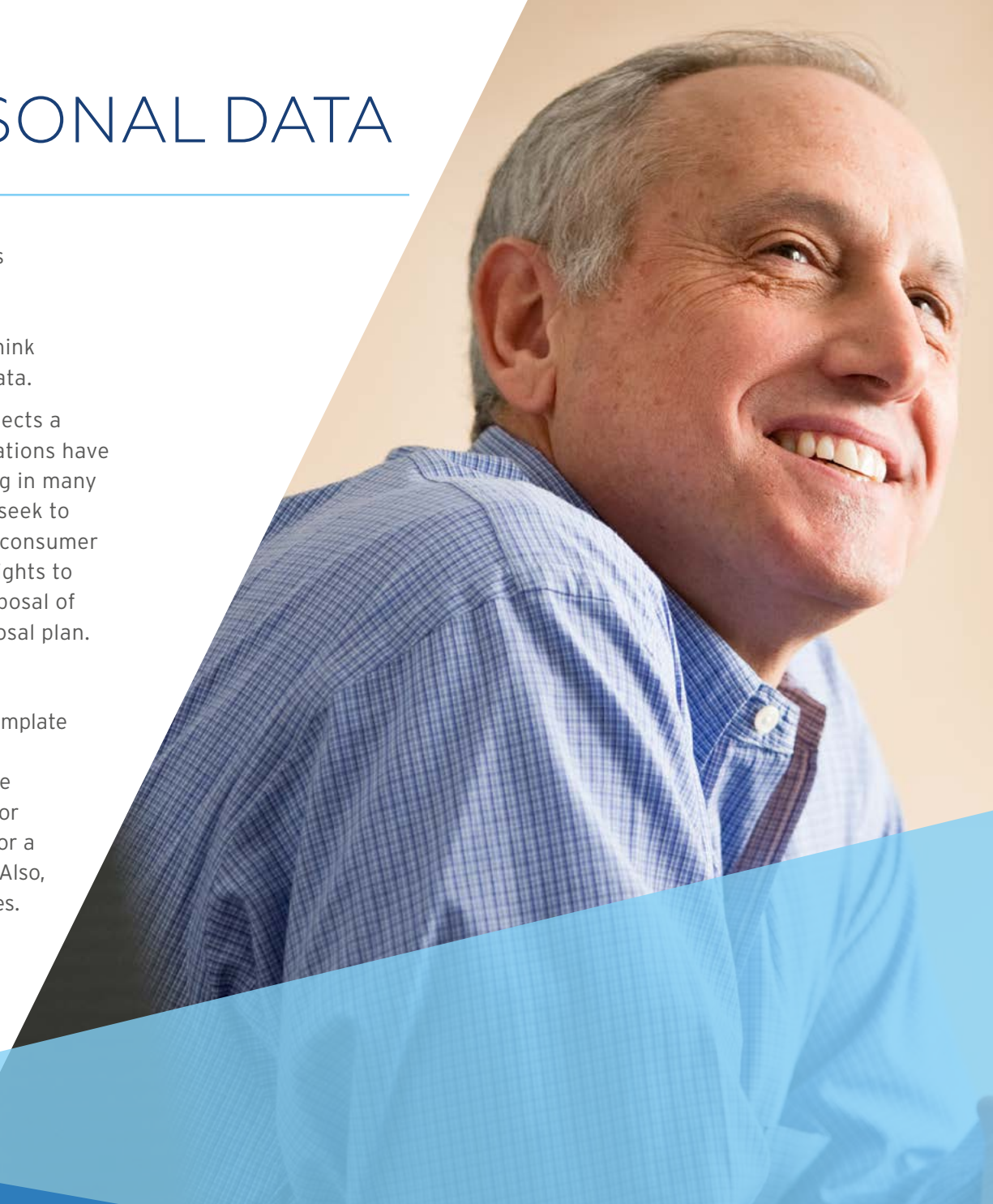
DISPOSAL OF PERSONAL DATA

Under the California Consumer Privacy Act (CCPA), consumers have the right to request the deletion of personal information from businesses that have collected it from them. This means that businesses subject to California's requirements need to think proactively about how exactly they plan to delete consumer data.

In some ways, the California Consumer Privacy Act (CCPA) reflects a mindful shift regarding personal data. Individuals and organizations have progressed from not thinking about it too much, to oversharing in many contexts, to protecting privacy today. But as more consumers seek to have their information deleted, entities subject to California's consumer privacy requirements and the organizations extending those rights to their entire customer base may need some extra help with disposal of personal data. Here are some tips to help build your data disposal plan.

REASSESS DATA DISPOSAL PRACTICES

Organizations may find that now is the appropriate time to contemplate their data disposal and recycling practices. "Data disposal" can mean a lot of things under various laws – it may refer to complete destruction or erasure, or it might refer to data's anonymization or de-identification. Legal requirements calling for data to be kept for a specified time period may complicate your data disposal efforts. Also, remember that data resides in both paper records and digital ones.



INSTITUTE A SHRED-ALL PROGRAM FOR PAPER

Organizations can spare their employees the frustration of deciding how the law's requirements apply to their documents by developing shred-all programs for paper. This way, an employee does not need to assess every document to determine if it includes personal or sensitive information. Instead, when a document has reached the end of its useful life, it will simply be sent to the shredder.

An organization's leadership won't need to worry about inappropriate materials being tossed in the general trash and found by people with less-than-noble intentions. Considering the possible liability of paper records making their way into the wrong hands, a shred-all program helps thwart any costly data breaches, and also removes subjective decision-making by employees about which records contain personal data. It's simple: Shred everything.

A records retention schedule and disposition management program is a critical component of the information lifecycle. Iron Mountain's Advisory Services team can help customize an organization's document retention rules. By leveraging Iron Mountain's Policy Center solution - which is now integrated with Iron Mountain InSight® and Workflow Automation™ powered by Hyland solutions - organizations can also automate document retention and improve compliance.

Whether shredding should be conducted on- or offsite is more of a business decision. Iron Mountain's Secure Shredding Services can be provided on- or off-premises, and special purge or bulk shredding is also available for organizations needing to destroy unnecessary materials that have been around for a while.

UPDATE E-WASTE DISPOSAL AND IT ASSET DISPOSITION PROCEDURES

In the same vein, digital data disposal procedures may merit a second look in light of California's new law and initiatives in other states that encourage more responsible handling of personal information. As businesses implement the CCPA's requirements and focus on the disposal of personal data, they may want to destroy digital data soon after any retention requirements have been met.

It's important that data is destroyed securely and within the bounds of applicable laws. If appropriate, some of that data may need to be anonymized. In the end, many businesses are grappling with their approaches to the disposal of personal data as they strive to adhere to California's requirements and those of other states.

CCPA is also forcing organizations to think about their technology disposal to ensure they aren't overlooking key security protocols and putting their organizations at tremendous risk. Iron Mountain's Secure e-Waste and IT Asset Disposition solution helps you destroy and recycle or repurpose various IT equipment types with secure, reliable, environmentally compliant services.

IN A PEW SURVEY,
90% OF RESPONDENTS
PREFER TO CONTROL
THE PERSONAL
INFORMATION THAT
IS AVAILABLE AND
USED BY BUSINESSES.

SOURCE: CALIFORNIA DEPARTMENT OF JUSTICE, INITIAL STATEMENT OF REASONS, PROPOSED ADOPTION OF CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

KEY TAKEAWAYS

Organizations are constantly pressured to comply with emerging regulations in an ever-shifting regulatory landscape. A strong information lifecycle will enable your organization to comply with privacy regulations, such as the CCPA.

From managing complexity and risk to providing automated governance, customers can rely on Iron Mountain's deep heritage and industry expertise throughout the information management lifecycle. To learn more about the topics discussed in this eBook, I encourage you to visit our [Privacy in the Information Lifecycle](#) page.



ABOUT IRON MOUNTAIN

Iron Mountain Incorporated® (NYSE: IRM) is the global leader in storage and information management services. Trusted by more than 220,000 organizations around the world, Iron Mountain's real estate network comprises more than 85 million square feet across more than 1,400 facilities in 46 countries dedicated to protecting and preserving what matters most for its customers. Iron Mountain's solutions portfolio includes records management, data management, document management, data centers, art storage and logistics, and secure shredding, helping organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information. Founded in 1951, Iron Mountain stores and protects billions of information assets, including critical business documents, electronic information, medical data and cultural and historical artifacts. Visit www.ironmountain.com for more information.

© 2020 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are the property of their respective owners.