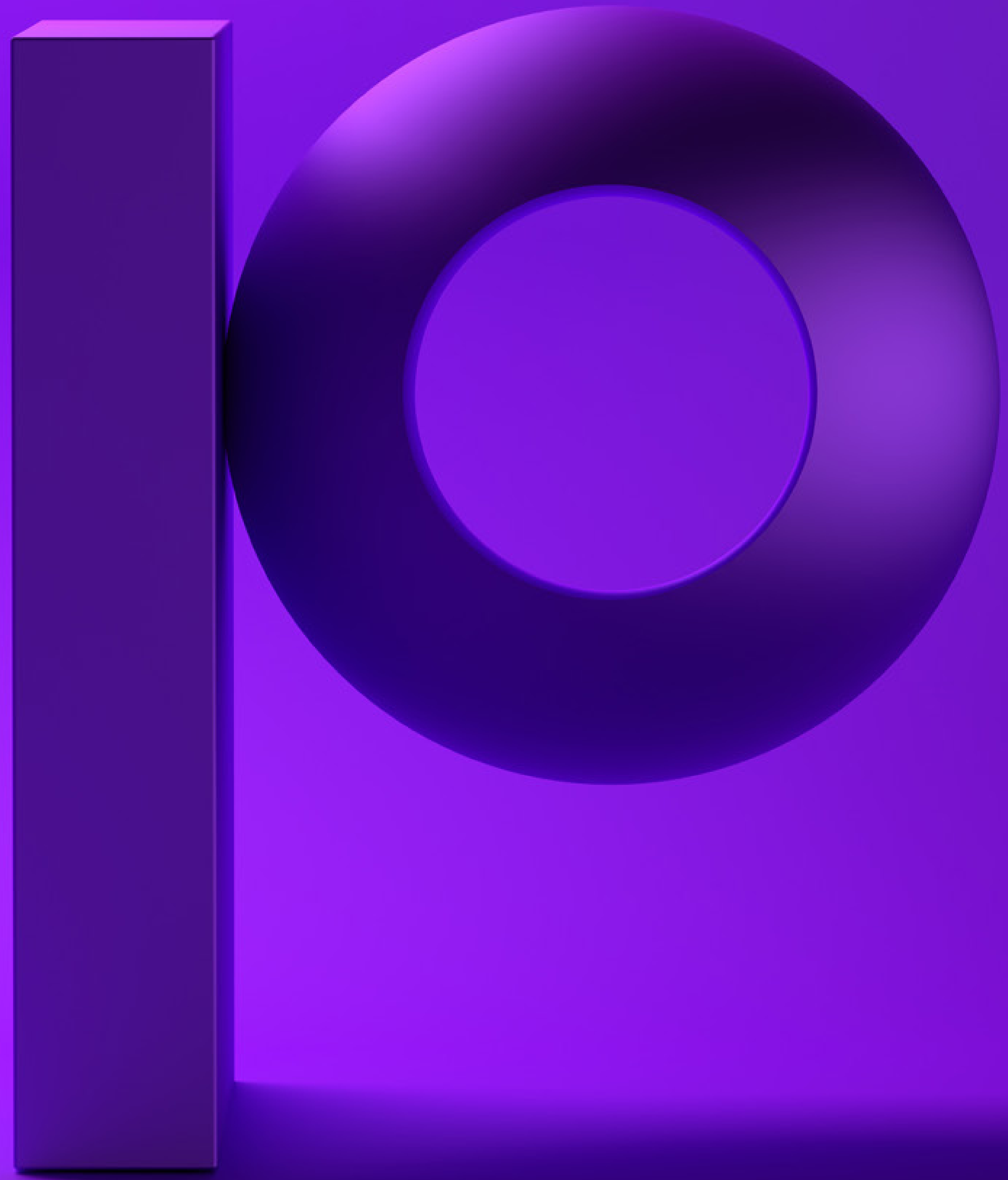
precisely

What the California Consumer Privacy Act (CCPA) and Similar Regulations Mean for You:

Addressing IBM i Data Privacy



Introduction

The California Consumer Privacy Act (CCPA) gives California residents numerous data privacy rights while penalizing organizations that are in violation. The law, which takes effect on January 1, 2020, groups these rights into five general categories:

1. The right to know what information is being collected
2. The right to know how personal information is being used
3. The right to opt out of the sale of one's personal information
4. The right to access a copy of one's personal information
5. The right to not be discriminated against by organizations when one exercises one's privacy rights

In addition to the above, CCPA puts pressure on organizations to protect California residents from having their personal data exposed by a data breach.

Thousands of organizations worldwide are affected by CCPA. That's because, regardless of whether or not the organization is located in California, the organization will be required to comply as long as it meets one or more of the following criteria:

- Annual revenue is greater than $25 million and the organization stores/processes data about California residents
- 50% of annual revenue comes from selling information about California residents
- Personal information is collected or purchased that affects 50,000 or more California residents

Comparing CCPA with GDPR

Many of the organizations affected by CCPA recently made large investments to get systems and processes in place to comply with the European Union's General Data Protection Regulation (GDPR) privacy laws. Fortunately, that investment should help those same organizations meet CCPA requirements as both regulations give individuals fairly similar ata privacy rights. A detailed comparison of the two laws can be found in numerous articles that a web search will provide.

Like GDPR, CCPA mandates that data about individuals be protected against a breach, and it gives individuals the right to sue for damages should a breach expose their data and that data wasn't encrypted or otherwise made unreadable. In addition to fines for noncompliance, the cost of these suits could be massive for an organization should thousands or millions of individuals be affected.

California: a legal bellwether for tech legislation

As the most populous state in the U.S. and the world's fifth largest economy, it's not unusual for California to be at the forefront of tech-related legislation that eventually triggers similar laws in other parts of the country. In 2002, California enacted the first data breach notification law, which was soon followed by 45 other states enacting similar legislation. With CCPA on the books, data privacy legislation is now pending in New York, Massachusetts, and Rhode Island, and other states are likely to follow. The possibility also exists that some sort of data privacy legislation might be enacted in the U.S. at the national level. Regardless of whether your organization needs to comply with CCPA or not, one or more data privacy regulations are likely to come your way. That's why the time to prepare is now.

Data Privacy Regulations and the Responsibility of IT Departments

For IT departments that need to comply with CCPA or any other data privacy regulation, there are typically two primary requirements that must be met: 1) have data management and reporting technologies/processes in place that make it possible for staff to efficiently fulfill consumer requests, and 2) have sufficient data security technologies/processes in place to prevent a breach, and should a breach occur, obscure any sensitive data.

Data management and reporting technologies/ processes for request fulfillment

Data privacy regulations make it critical that organizations are able to identify all of the ways in which they collect, use, sell, and share personal information. Remember, CCPA gives individuals the right to know the data that is collected about them, know how that data is used or sold, receive a copy of that information, and have that information deleted upon request. To meet these requirements, an organization must efficiently respond to these requests, which means having sound data management systems and processes. And if your organization uses service providers to store or process this data, your compliance efforts must also extend to these entities.

Security technologies/processes for preventing breaches and obscuring data

As if organizations needed it, CCPA stacks on yet another reason why it's critical to properly secure data from unauthorized access. In addition to preventing a breach that could expose personal data, it's equally critical that sensitive data is obscured; i.e., made unreadable through encryption or another technology should a hacking incident occur.

The remainder of this eBook will explore strategies for both preventing a breach of IBM i environments and ensuring that sensitive data is properly obscured in the event of a breach.

Obscuring Sensitive IBM i Data

Sound IBM i security practices and technologies are critical to preventing the occurrence of a breach, but if it does happen, it's equally critical that sensitive data cannot be read by the unauthorized actor. As mentioned in the introduction of this eBook, CCPA gives consumers the right to sue an organization in the event of a data breach that exposes their personal information if that data wasn't encrypted or otherwise made unreadable. In addition to encryption, CCPA mentions "redaction" and "deidentification," which could be accomplished through tokenization (also called pseudonymization), anonymization, and masking.

Encryption

Encryption transforms human-readable data into unreadable ciphertext by taking a publicly available algorithm and combining it with a private encryption key (a unique, secret sequence of bits). When the data needs to be read by an authorized party, it must be decrypted using the proper encryption key. For encryption to be effective, it's critical to carefully manage and protect encryption keys; if your keys are found by a hacker, your encryption efforts could be for naught. In fact, if your data is encrypted and there is a breach, you will likely need to show a compliance auditor that encryption keys were adequately secured.

Encrypting data at rest

Third-party encryption solutions for IBM i are used to encrypt sensitive data "at rest" (the data resides in some form of storage). Before V7R1 of the operating system, encrypting data at the field level within databases required application changes in order to call encryption APIs. Today, however, application changes are not needed thanks to IBM adding a column- or field-level exit point called Field Procedures (FieldProc). Third-party encryption solutions provide exit programs that can be called by the FieldProc exit point to encrypt and decrypt at the field level without application integration projects. Additional IBM i objects such as IFS files or backup files can also be encrypted through command lines or APIs.

Encrypting data in motion

It is essential that the transfer of personal data over a network, whether as streams of data or entire files, be encrypted to prevent this data from being exposed should it be intercepted by a bad actor. When data streams are sent, they are typically encrypted by technologies embedded within network protocols, such as encrypted Telnet, HTTPS, etc. When entire files are sent between servers or entities, this is typically done using SSH Secure File Transfer Protocol (SFTP) or FTP over SSL (FTPS). Third-party managed file transfer solutions help execute and manage these secure file transfer processes and can also encrypt data at the source and target using PGP to prevent unauthorized access before or after the file is transferred.

Additional methods of obscuring data

Other technologies besides encryption can be utilized to make sensitive data unreadable to an unauthorized party. In essence, these technologies replace sensitive data with non-sensitive substitute values.

Tokenization

Referred to as pseudonymization by CCPA and elsewhere, tokenization replaces sensitive data with non-sensitive replacement values (tokens). The technology utilizes a database called a token vault to store the sensitive data along with information about the relationship between the sensitive data and its replacement token. By tokenizing the data on production systems and storing the original data within a token vault on another server, the production server is effectively removed from the scope of compliance. Of course, the token vault must be aggressively secured from breach, which is why many companies encrypt the contents of the token vault. Because there is no algorithmic relationship to the original data (as there is with encryption), there is no way to crack the token value to derive the original data. Third-party tokenization solutions for IBM i are available to automate tokenization and detokenization processes.

Anonymization

As a form of tokenization, anonymization permanently replaces sensitive data with a substitute value, making the original data completely unrecoverable. Anonymization is never used for production data, although it can be used on a copy of that data when it's needed for development or test environments. When data needs to be sent to a third party for reporting and data-aggregation purposes, anonymization can be used to remove any personally identifying information before it is sent.

Masking

Not an encryption or a deidentification technology per se, masking is instead used in conjunction with encryption and tokenization solutions. This technology obscures portions of a database field with an "X," an asterisk, or another designated character when that data is decrypted or detokenized to ensure that the application user sees only the data required to accomplish their job. The type and length of the mask that's used can vary based on the user and the context in which the data is being viewed.

Read the following Precisely eBooks to learn more about technologies for obscuring sensitive data:

- Encryption, Tokenization, and Anonymization for IBM i: A Quick Guide to Protecting Sensitive Data
- IBM i Encryption with FieldProc and Assure Encryption: Protecting Data at Rest
- The Essential Guide to Secure and Managed File Transfers on the IBM i

Protecting IBM i Systems from a Breach: The Importance of a Multi-layered Approach

In addition to obscuring sensitive data so it's rendered unusable should a breach occur, from a CCPA perspective it's equally important to prevent a breach from happening in the first place. A skilled intruder might break through a single security approach or technology and gain unauthorized access to systems and data, but when multiple layers of security are in place, hacking becomes much more difficult. That's why IBM i shops need a defensive posture that addresses each potential type of attack. Beyond the general IT essentials of physical security, network security, IT security policies, and periodic risk assessments, there are several critical IBM i-specific layers of security that must also be implemented.

Configuring security in the IBM i OS

Strong IBM i security requires proper configuration of the IBM i OS and related resources. This includes appropriate settings for system values, object permissions, user authorities (more about this shortly), and more. In addition, it's critical to keep OS versions and PTFs up-to-date.

Comprehensive access control

Traditional object-level security on IBM i is insufficient when it comes to protecting access from network protocols (e.g. FTP, ODBC, JDBC, OLE DB, DDM, DRDA, NetServer, etc.), open-source database access protocols (e.g. JSON, Node.js, Python, Ruby, etc.), and commands. IBM provides exit points for each of these access vectors, which can be utilized by rules-based exit programs to reduce the possibility of intrusion.

Taking control of logon security (beyond implementing strong password policies) and controlling access to elevated authorities are also important steps toward preventing external and internal parties from accessing sensitive data. Multi-factor authentication strengthens logon security by requiring users to provide one or more additional identifying factors beyond username and password before accessing systems, objects, commands, etc. Tight control of users' abilities to obtain powerful authorities is best done by giving users only the authority they need to do specific tasks for a limited amount of time and within strict parameters (i.e. time of day, IP address, etc.). Revoking that authority after the specified time is key to maintaining control.

Third-party solutions are available that streamline the management of each of the above access control strategies.

Learn more about IBM i access control in these Precisely white papers:

- **Four Powerful Ways to Use Exit Points for Securing IBM i Access**
- **Managing Elevated IBM i Authorities: Best Practices in Data Security and Compliance**
- **Multi-Factor Authentication for IBM i**

Security auditing and monitoring

Quickly spotting suspicious activity is vital to preventing a breach or at least minimizing damage should one occur. That's why putting in place tools and processes that provide comprehensive auditing and monitoring of IBM i activity is another important layer of security.

In addition to tracking activity through system message queues and QHST entries, IBM i shops can utilize the journaling capabilities of the operating system to record a rich layer of system activity. This unalterable information makes it possible to log and trace user authentication, system access, data changes, object configuration changes, and more. The output from journaling is both prolific and cryptic, but third-party solutions greatly simplify and automate the analysis of journal activity to pinpoint suspicious events, as well as to trigger alerts, create reports for auditors, and more. For organizations that use an enterprise-wide security information and event management (SIEM) solution to aggregate and analyze security activity across disparate IT systems, third-party solutions are available to forward IBM i security information to a SIEM.

Organizations that keep particularly sensitive information can go beyond analyzing the database changes tracked in log files and actually monitor user views of Db2 data. Knowing whether an unauthorized user viewed sensitive data is something that journaling can't track. Third-party IBM i security solutions are beginning to offer this capability.

Learn more about protecting your IBM i through a multi-layer approach in the Precisely white paper The Essential Layers of IBM i Security.

Get a Head Start Toward Better IBM i Security

As stated at the outset of this eBook, the time to prepare for data privacy regulations is now. Even if your organization isn't affected by CCPA, it's likely that one or more data privacy regulations will affect you in the not-too-distant future. In order to get a head start toward complying with these regulations, your organization must:

- Know where data about individuals is located within your systems
- Be able to respond efficiently to requests from individuals
- Harden the systems containing this sensitive information against a breach
- Obscure sensitive data in the event of a breach

But regulations aside, given the significant cost and disruption of a data breach, it is only prudent that every organization make regular improvements to its IT security. That's why the goal of this eBook, as well as the other Precisely eBooks and white papers mentioned on the previous pages, is to give you a road map that guides your journey toward more secure and resilient IBM i environments.

Precisely Can help

With best-in-class IBM i security solutions and services, Precisely stands ready to help you strengthen IBM i security as you work to comply with CCPA and other regulations.

Precisely Security Software for IBM i

Our proven software solutions cover many critical areas of IBM i security, including:

- Security risk assessment
- Compliance monitoring and reporting, with SIEM integration
- Monitoring of user views of sensitive data
- Multi-factor authentication
- Elevated-authority management
- Exit point control of network access, open-source access, database access, and command usage
- Encryption and key management
- Tokenization, anonymization, and masking
- Secure file transfer

Precisely Professional Services for IBM i

Our security experts stand ready to help you reinforce IBM i security and meet compliance requirements in numerous ways:

- Security risk assessment services
- Compliance/security audit assistance
- Managed services for Precisely's security products
- Security technology installation and training

To learn more about Precisely's security products and services, visit www.precisely.com

precisely