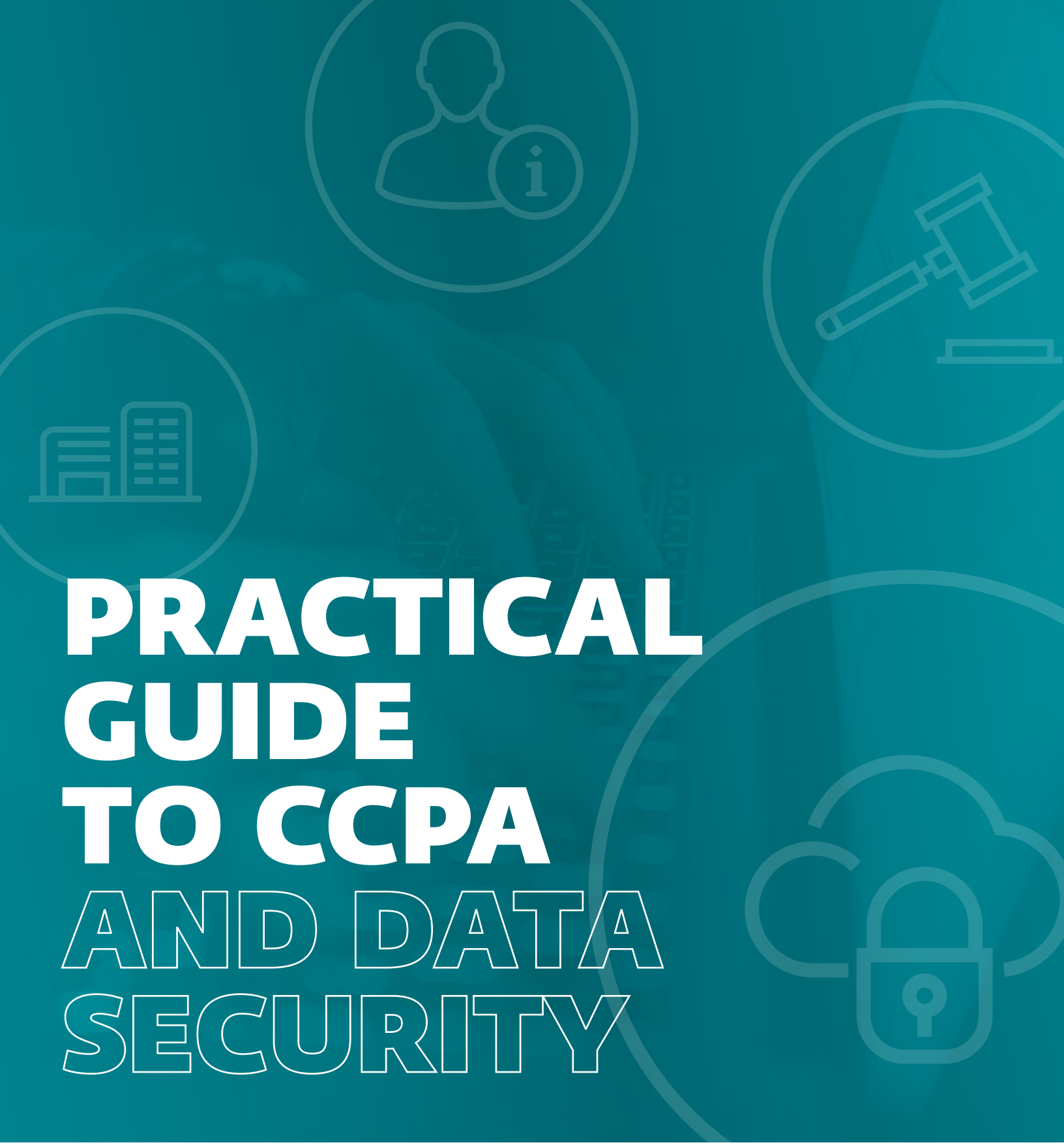

PRACTICAL GUIDE TO CCPA AND DATA SECURITY

ENJOY SAFER TECHNOLOGY™

AUTHORS:
Tony Anscombe, Lysa Myers and other ESET experts // August 2019

TABLE OF CONTENTS

Introduction

The global trend toward privacy legislation has reached the U.S., in the form of the California Consumer Privacy Act (CCPA). This sweeping piece of legislation was signed into law in June 2018 and impacts many more businesses than is generally understood. It gives new rights to control the use of personal data to 40 million residents of the state of California. But the impact and scope reach well beyond California's borders. The provisions of the law extend to companies doing business or collecting personal data about California residents, impacting an estimated half a million businesses in the U.S. alone.

We've put this paper together as a practical guide to the act. Our goals are to:

- Help you understand whether you're bound by the act, and your obligations under it
- Provide an overview of how the act compares with the General Data Protection Regulation, the EU's privacy regulation, which also applies to many U.S.-based companies
- Explain the potential penalties and risks of non-compliance
- Provide guidance into how to implement "reasonable security," a key requirement of the act

The CCPA: Overview and impact

The CCPA is a game-changer for the way it puts control over private information into the hands of consumers. Compared to any other privacy regulation applicable in the U.S., the definition of private information is more sweeping. The leeway given to consumers to control their information is broader. Their avenues for taking action or seeking remedies are wider. And the penalties are potentially very large. Moreover, privacy advocates anticipate that the law will be a model for similar legislation in other states, perhaps leading the federal government to impose its own regulations nationwide.

As an information-security company, we want to ensure our customers are equipped with the right knowledge to understand the impact this law may have on their businesses. The security requirements are nebulous and some are yet to be clarified by the state Attorney General's office. In some cases, we may only learn about the true meaning of some of the provisions by example — that is, through enforcement actions. As security practitioners, we believe that the intent of the bill is a net-positive: to protect against data breaches that would expose individuals' personal data. But the law's reliance on the as-yet undefined "reasonable security" standard can put companies subject to the regulations in limbo. For this reason, ESET has put together guidance based on our expertise and best practices in the cybersecurity industry. You can leverage them to feel confident in your security vis-à-vis the act. See section four for details.

Here are just a few of the impacts the CCPA will have.

The definition of personal information will never be the same

There are two broad categories of personal data recognized by the act.

The first category is personally identifiable information as understood by many, defined in the pre-existing California civil code. The security and data breach aspects of the CCPA deal with this type of information. It includes:

An individual's first name (or first initial) and last name, combined with one or more of the following:

- Social Security number
- Driver's license or California identity card number
- Account number, credit or debit card number, in combination with the security code, access code or password permitting access to that account
- Medical information
- Health insurance information

If *either* the name *or* the associated data is not encrypted or redacted, exposure is considered an actionable breach under the act.

The second category is a greatly expanded definition of personal information, aggregated and defined for the first time in the CCPA. The consumer privacy and control aspects of the CCPA deal with this category of information. It is any information that identifies, relates to, describes, or is capable of being associated with a natural person, including:

- **A broad scope of demographic, social and financial information** including real name and alias, postal address, telephone number and signature; social security, driver's license, passport and insurance policy number; bank, credit and other financial account number; online identifiers such as account name, unique personal identifier, IP and email address; information about education and employment.
- **Commercial information** including records of personal property, product or service purchase, review or history of consideration.
- **Classifications that are protected under California or Federal law** including race, national origin, ancestry and religion; physical or mental disability or other medical condition; marital status, sex, age and sexual orientation.
- **Health insurance data and medical information.**
- **Geolocation data.**
- **Internet or network activity information** including but not limited to browsing history and search history, and information about interaction with an application, website or advertisement.
- **Biometric data** including biological or behavioral characteristics; DNA; iris or retina image; finger, hand and palm print, facial recognition and vein patterns; voice recordings; gait patterns and rhythms; keystroke patterns and rhythms; sleep, health and exercise data.
- **Audio, electronic, visual, thermal, olfactory, or similar information.**
- **Inferences drawn from any of the above information** used to create a profile about a consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence and aptitudes.

Protections extend to millions

The CCPA protects participants in the world's fifth-largest economy — the 40 million residents of California. While businesses may still collect and use personal data, CCPA gives California residents a number of rights to know how and what data is collected, sourced, used and shared, to deny sale of their data or to dictate its deletion, and to take action when their personal data is breached.

Where your business is based doesn't matter

The act applies to any for-profit business that "does business" in the state of California. While "do business" isn't defined in the language of the act, our understanding is that it applies to any business that is physically located either inside or outside of California and that collects and handles information about California residents. That includes businesses that engage others to collect information for them, or collect information on behalf of others. "Collect" is defined in the act as buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

You are bound by the act if you 1) are a for-profit business, 2) collect personal information, 3) do business in California, and 4) exceed one or more of following thresholds:

- Have gross annual revenues in excess of $25 million
- Buy, receive, sell, or share personal information from 50,000 or more consumers, households, or devices
- Derive 50% or more of annual revenue from selling California residents' personal information

Small and medium-size businesses may be at risk

The broad definition of personal information under the act is without precedent. Under the second criterion above, many smaller businesses are expected to be subject to the act. A business with a website that collects and retains personal data from just 137 California visitors per day could be subject to the CCPA.

If you fall under the act, the range of statutory penalties and the dollar amounts, as described in section four, would apply equally to a family-owned business and to a very large corporation. Especially if you store a very large amount of consumer data relative to your staff resources, you're actually at greater risk than a big company in your ability to weather the storm. The time and costs of dealing with a large volume of consumer inquiries could place a huge burden on your company. A data security breach is an even bigger threat. Such events, when they happen, are unexpected. You can't plan for them, you can only prevent them.

Regardless of business size, you would do well to determine now whether you are subject to the law or if larger business partners will require you to comply. If so, you can begin assessing the data you handle, identifying compliance gaps, preparing a roadmap and implementing. See section five for ESET's guidance.

The deadline is now

Companies must comply by January 1, 2020. As of that date, consumers may begin requesting information as required under the act. They can also seek actual damages or statutory damages, individually or as part of a class-action, for a data breach. The act also provides for enforcement action by the Attorney General, which can begin either six months after publication of the final regulations or July 1, 2020 — whichever is sooner.

This doesn't mean you can wait until January 1, 2020 to do anything. You must be able to provide information about data dating back 12 months from the compliance date. Bottom line? If your business is subject to the act, you need to examine your processes for storing and handling personal information now, and be ready to act on requests and respond about data collected, stored, processed, shared or sold retroactive to January 1, 2019. You also need to ensure that your security procedures and practices are up to par, before the January 1, 2020 date when you'll be exposed to liability for a data breach.

If you wait, it's too late

You need to have visibility to any personal data collected, stored, processed, shared or sold from January 2019 forward to comply with the act, once it goes into effect.

CCPA and GDPR: The same, but different

You may have seen the CCPA referred to as "California's GDPR," or some similar phrase. While the two bodies of regulation may be similar in their intent to protect individuals' personal data collected and sold by businesses, they differ in significant ways.

1. Who must comply

Arguably the biggest difference between GDPR and CCPA is in who must comply with the regulation and whose data is covered. GDPR applies to any company that sells products or services to "individuals" in the EU. "Individuals" means not only citizens of the EU, but also people who are using those products or services while temporarily based in those countries. By contrast, CCPA excludes people traveling to California, but the protections do still apply when a California resident is traveling elsewhere.

Given that California is one of the most populous states in the US, many companies do business with its residents. Companies that exceed certain thresholds fall under the provisions of the CCPA; we covered those in section two. The thresholds do limit the number of businesses that will be required to comply with CCPA. Considering that one of the objections to GDPR after its first year in effect was how it disproportionately affects smaller businesses, the exceptions could be considered a way of addressing that complaint.

This is not to say that smaller businesses should be less wary about the prospect of being attacked, or that they can afford to be less protective of personal data. Smaller businesses may also have less ability to withstand losses due to the theft of personal data.

And it's worth noting that larger companies will require smaller ones to comply with CCPA's regulations if they do business together. As we've seen in far too many recent security breaches, companies often inherit the risk of businesses they partner with.

2. How penalties are applied

Both CCPA and GDPR have two-tiered penalty structures for non-compliance, as a means of indicating different severities of incidents. In the case of GDPR, this is based on which articles have been violated by the organization that's been breached: up to €10 million, or 2% annual global revenue – whichever is greater; or up to €20 million, or 4% annual global revenue – whichever is greater.

The GDPR fine amount can be further modified depending on a variety of other factors. For example, if there is evidence that this was an unfortunate incident that happened to an otherwise well-prepared organization, and actual harm was mitigated by protection measures, the fine may be decreased. If this event appeared to be due to negligence – especially repeated offenses – or if the privacy incident was intentional, the fine may be greater. The sensitivity of the data lost may also affect fines.

For the CCPA, the two tiers are capped at $2,500 "per violation" for unintentional incidents and $7,500 for intentional violations. The act also allows California residents to file a lawsuit against companies that have experienced a data breach involving personally identifiable information as defined by the California civil code. We cover the CCPA penalties in more detail in section four.

PER VIOLATION

$2,500
unintentional incidents

$7,500
intentional violations

3. The right to data deletion

Both GDPR and CCPA offer covered consumers the right to request that their personal data be deleted. There are naturally limits to an organization's ability to fulfill this request. They can't delete your address data for a purchase they've agreed to ship to you until after the transaction is completed, or remove data that otherwise needs to be retained for legal reasons, for example.

But the way CCPA views data that is eligible for deletion is slightly different: consumers can only request deletion of data that is collected from them. Data that is gathered from another source, such as being purchased from a third party, is not included. This is clearly a much smaller subset of personal data than is covered in GDPR, as data brokers gather quite a bit of data about each and every one of us.

4. Approach to "informed consent"

Informed consent is an important component of GDRP and CCPA, as it is meant to ensure that consumers have a clear idea of what they're agreeing to when they share their personal information with a business. In both regulations, there is an expectation that organizations will clearly spell out what will be done with consumers' personal data. The specifics beyond that get a little more complicated.

GDPR requires organizations to explain data-gathering policies at the time of collection so that consumers can opt in. CCPA requires organizations to explain their policies at or before the time of collection so that consumers may opt out. This means that the placement of the explanation in relation to the area where consumers share their data may be significant. But with CCPA, it also requires that there be a clear and conspicuous link entitled "Do not sell my data" that allows consumers to opt out without first having to create an account.

5. Data portability

While both GDPR and CCPA require businesses to share personal data with consumers upon request, only GDPR requires those businesses to share personal data with another data controller upon request. That is to say, if you request data from one phone company as you prepare to switch to another provider, with CCPA you would have to then give that data to the new provider yourself, rather than it being handed directly from the old provider to the new one.

6. Requirement for a Data Protection Officer

One area where CCPA differs significantly from GDPR is in the former's lack of a requirement for a Data Protection Officer. In the EU regulation, it's required to appoint someone whose role is specifically to coordinate secure and sensible data handling within an organization; in the California regulation there is no such expectation. The GDPR's requirement ensures that there are adequate resources allotted to make sure an organization is well prepared to deal with the challenges that come with properly managing data. Without this resource, companies that are trying to get up to speed on complying with CCPA may struggle. We recommend instituting a similar role, as we explore in section five.

7. The concept of "household" data

Most of us are used to thinking of "personally identifiable information," which is data that can be used to identify us individually. But many of us share devices or services in a way that makes it less "personally" identifiable, but it still creates a unique profile of each user. As savvy as companies are becoming about using data to fingerprint individual users, it's entirely possible that "household" data could be parsed out to separately identify each individual. It's an interesting and potentially forward-looking addition to require the protection of both individual data as well as the shared data of those who share living arrangements.

What the differences mean

If you're a U.S.-based company with European customers, you've already had to deal with GDPR compliance (or you should have). It's true that both CCPA and GDPR share a similar intent, and certain features. But it's not necessarily automatic that if you're compliant with GDPR, that you're also compliant with the CCPA. The good news is this: If you are GDPR-compliant, when you go through your CCPA requirements, you'll likely find that you're a lot further along because many of the boxes have already been checked.

If you've been through GDPR, CCPA changes the privacy landscape yet again. There are enough differences between these two sets of regulations that you need to consider each one separately, and prepare accordingly. By taking time to review now, before CCPA goes into effect and you're faced with the reality of dealing with consumer inquiries under the act, your organization can avoid unpleasant, costly surprises.

CCPA ≠ GDPR

Even if you have already complied with GDPR, the regulations are different. Treat CCPA compliance as a separate exercise.

Considering the consequences: Risks and penalties

You've probably heard stories of large organizations getting hit with multi-million dollar fines, or suffering loss of goodwill due to stolen customer data. Most often, these have been large retailers or others who process credit cards, or healthcare organizations required by law to protect private medical information. If your organization falls under the CCPA, no matter the industry, you're now in the crosshairs, too. That's because the definitions of private information are so much broader and your obligations more complex.

Our goal is to keep you out of trouble. We include the following information so you understand the risk of non-compliance with the CCPA, so you can plan accordingly. There are two types of actions possible if you're found to be in violation of the CCPA.

Action by the California Attorney General

If you violate any provision of the CCPA, after you've been given a 30-day notice and an opportunity to "cure" the problem, the law specifies civil penalties of up to $2,500 "for each violation" or $7,500 "for each intentional violation." However, it is unclear exactly what constitutes a single violation. A single incident that impacts multiple consumers could constitute one violation, or each consumer impacted could be penalized as a separate violation. This question represents a huge difference in potential risk exposure; the Attorney General is expected to issue draft guidance in the fall of 2019.

DRAFT GUIDANCE EXPECTED FROM ATTORNEY GENERAL

FALL 2019

The following violations could lead to action by the Attorney General. All of them except the last could be triggered when the type of information involved falls under the CCPA's expanded definition of private information (see section two). These include failure to:

- Inform consumers about the types of personal information that you are collecting
- Inform consumers that their personal information is being sold or disclosed, the type of information, and who has received it
- Delete consumers' personal information on request
- Refrain from discriminating against consumers who have exercised their rights under the act
- Disclose how your company will use personal information
- Give consumers the option to opt-out of having their information sold or shared to others
- Implement "reasonable security" measures to protect against personal data breaches as explained in the next section (applies only to the narrower definition of personally identifiable information under the California civil code)

Action by individuals or classes of consumers

If you experience a breach of unencrypted or unredacted data involving personally identifiable information as defined in the California civil code (described in section two), caused by your failure to implement "reasonable security," consumers can now take direct action under the law. You have 30 days to "cure" the violation and notify the consumer. If not, individual consumers exercising this right of action can exact statutory damages of between $100 and $750 per incident or actual damages — whichever is greater. A few items to note about consumer actions under the CCPA:

- With the statutory penalties of $100-$750 per incident, individual consumers don't have to show or prove they incurred actual damages — the mere fact that the breach occurred is enough.
- The language of the act is "class-action friendly," raising the prospect of thousands of consumers taking part in class-action lawsuits seeking the statutory damages.
- A company with information on 10,000 consumers could face up to $7.5 million in potential risk exposure depending on the nature of the information disclosed in a breach.

It's worth a reminder that the act is a moving target, and is subject to further amendment. And certain elements in the act will require further clarification. One of them is what constitutes "reasonable security," which we cover next.

Higher cyber-stakes

If you store driver's license, Social Security, bank account or credit card numbers, or medical or health insurance information, CCPA's class-action provisions significantly increase your risk exposure.

ESET's guide to "reasonable security"

Cybersecurity is a moving object, it is not a do-and-done activity. Information security is a process that needs to be developed, implemented, monitored and regularly updated. And there is no such thing as perfect security. CCPA states that you need "reasonable security," but the definition of reasonable can be different for every person whether a lawyer, judge, consumer or vendor.

Until the legislation takes effect and the first cases are brought to light, the precise definition of "reasonable security" may continue to be murky. In the meantime, our view is that the best approach is to draw from the definitions, requirements and suggested best practices that already exist. A number of organizations offer guidance on risk management, process, policy, and managing and controlling systems and information. Some of the best are:

CIS Controls by the Center for Internet Security. You might know this list as the SANS 20. The *California Data Breach Report*, issued in February 2016 by the California Attorney General, stated that "failure to implement all 20 [controls] that apply to an organization's environment constitutes a lack of reasonable security." It is unknown whether this will be the standard declared specifically for CCPA compliance.

Start With Security: A Guide for Businesses, published by the Federal Trade Commission. The guidance and broad recommendations are particularly valuable, as they are drawn from the FTC's experience with actual data breaches and settlements.

NIST Special Publication 800-171, published by the National Institute of Standards and Technology. This publication or an alternate, *NIST Framework for Improving Critical Infrastructure Cybersecurity*, were proposed as the standard for "reasonable security" in an amendment to the CCPA. The amendment failed, leaving "reasonable security" as the standard, but both publications are highly authoritative.

In practice, we drew largely from the FTC's recommendations, buttressed with the best practices across all three publications and our own experience. While we are not lawyers — we are technologists — this is our practical guidance on how your organization may achieve "reasonable security."

1. First and foremost: Know your data

Start with the data itself. Every company collects data regardless of how big or small they are or even what business they are in. Suppose you're a contractor storing customer phone numbers in your phone. That is data collection that includes personal information. Unless the phone contains 50,000 names, that's far below the threshold required by the act. But what about a large contractor with 200 employees, with 250 names in each phone? That's 50,000 — meeting one of the thresholds and making the company subject to the act.

Here's what's important: Personal information can be and is stored everywhere. It may be challenging to understand what personal information exists, where it resides, who has access and for what purpose. But you first need to take a thorough look at your data to understand which of the two categories it falls into (see section two) in order to understand how it should be treated and protected under the act.

2. Don't hoard data you don't need

Data that you don't have is data that you don't need to protect from being breached.

- **Don't collect personal information needlessly**. Consider the personal nature of the information that is being collected and the damage that it can cause if the data enters your environment.

- **Hold onto information only as long as you have a legitimate business need for it.** The ease with which data can be collected and inexpensive storage has caused many companies to collect and store data on the basis that one day they might need it.

- **Don't use personal data when it's not necessary.** Both the GDPR and CCPA require there to be a sound business reason to collect and store the data.

Purging non-essential information assists in complying with privacy requirements and mitigates risk to the business. It also ensures that the data you use is fresh and relevant. If you send an irrelevant email to a customer who purchased something from you once, five years ago, you'll only frustrate that customer.

3. Appoint a Data Protection Officer

To bring focus to the where, what and why of data and the need to protect it, the GDPR requires companies to appoint a Data Protection Officer (DPO). The DPO is primarily responsible for overseeing the company's data protection strategy and compliance with GDPR. As we noted earlier, the CCPA does not require a DPO or similar role, but in our opinion the GDPR got it right. A large part of the challenge to being or becoming compliant is knowing who is responsible for data collection. If you have distributed the responsibility, then nobody is responsible.

The DPO's responsibilities under the GDPR include, but are not limited to, the following:

- Educating the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR supervisory authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information

With someone responsible in place, fulfilling the rest of the following items becomes simpler, at least in principle.

4. Control access to data sensibly

If your company relies on a unique recipe or other piece of information, then it's likely very few people are privy to knowing what the secret sauce is. Data should be treated in the same way. Only those who need to know or have access to the sensitive or personal information contained in data should be granted access to it.

The DPO or person in control of the data should categorize the data, allowing an access policy to be created so that only certain employees are granted access based on their business need.

The policy should go further and may limit where and from what devices individuals can access information. If you have nomadic sales warriors running around the country prospecting for customers, then access to data that isn't directly essential or personally sensitive can be blocked by policy, ensuring that data is not stolen from a remote device.

Trust in the data/network administrators to control access to these sensitive company assets, but don't forget to limit their access too. Not all administrators need to be able to see the data or be able to grant access. Put controls in place to control the controllers.

5. Require secure passwords and authentication

This particular topic never seems to be far from the conversation of cybersecurity. In April of 2019 the UK's National Cyber Security Centre (NCSC) found that 123456 was the most widely used password on breached accounts. The NCSC analyzed data from 23 million breached accounts and found that the top five also included 123456789, 'qwerty', 'password' and 1111111.

Hopefully, if you are reading this paper then you already have a password policy in force which requires upper and lower case, numbers, special characters and the like, with the requirements to change the passwords frequently and to stop previous passwords from being used again. Protect against brute force attacks — repeated attempt to input passwords — by limiting the number of retries.

Consider implementing strong authentication — a best practice whenever you're faced with regulatory compliance. Two-factor authentication is used by a variety of services today. For example, to access your bank account or execute a transaction might require you to enter a code sent to either an email address or phone. To use an ATM, you need both the card and the PIN. Using a physically separated device, such as a phone, for a second authentication factor in addition to a user name/password creates the two factor environment.

As technology advances, facial recognition, biometrics and even artificial intelligence are all playing a role to ensure only the authorized person is being granted access. As this area evolves and new methods are adopted, it's important to remain open to adding or changing policies to encompass them.

Lastly, as the FTC paper cited earlier says: "Locking the front door doesn't offer much protection if the back door is left open." It's important that all access methods are tested, security patches are installed on all software involved, and that there is monitoring in place to ensure there is no unauthorized access.

6. Don't store passwords in plain text

In addition to requiring strong passwords, pay attention to how you store them. It's your responsibility to store passwords securely as part of your customers' personal data. In the unfortunate circumstance of a data breach, the perpetrator could use the improperly stored password to masquerade as your customer to access your systems, and possibly accounts on other companies' systems if the customer uses the same password. This escalates the effect the breach of your system has on the consumer.

For security reasons, store passwords in hashed form, or even better, hashed and salted. This process stops anyone with access — approved or unapproved — from being able to see the actual password.

Here's how it works. When a user creates a password, it's passed through an algorithm and is transformed through what is commonly referred to as a "hash function." This turns the original text into a different set of letters and numbers that represent the password, stored in your database as a sort of fingerprint. Whenever the user logs in and enters the password again, it goes through the hash function and it's the hashed versions that are compared.

Salting complements hashing by adding another piece of data to the process of creating the hash. This further protects the stored passwords. Hashed or hashed-and-salted passwords are useless to a perpetrator if stolen, because the process is nearly impossible to reverse-engineer.

7. Store sensitive personal information securely and protect it during transmission

Encrypt everything.

A laptop left on a bus or taken from a car, a USB memory stick lost, or an email sent to the wrong person are all examples of why "encrypt everything" is a good starting point when thinking about what needs to be encrypted.

Encryption can be applied to both data in transit and data at rest. Data in transit, sometimes referred to as data in motion, is data travelling between devices — for example, from a device to the cloud, or from an endpoint to a corporate server. Data at rest is data that is stored on a hard drive, laptop, flash drive or other storage device.

Regardless of whether the data is at rest or in transit, unprotected data leaves businesses vulnerable to attack, either by malware or from an attacker attempting to steal the data. The ease and popularity of memory sticks also opens windows of opportunity that need to be addressed through policy. Ensure that any data being transferred on a portable device is protected in the right way, or alternatively not permitted at all.

Use strong encryption with industry-recognized algorithms and think through how to implement and manage it correctly. A robust method of key management is a must. Deploy an endpoint encryption solution that provides the ability to manage encryption keys remotely, and set policy for files, hard drives, portable drives, memory sticks and emails.

8. Segment your network and monitor who's trying to get in and out

There are many reasons to segment a network: reduced congestion, access control, security and resilience. A guest Wi-Fi network is a perfect example of network segmentation that addresses all of those goals. Visitors are untrusted and there is little or no control on the configuration of their endpoint devices, so you want to separate them from the corporate network.

The segmentation principle applies within the corporate network as well. Place sensitive data on servers that are separated, and implement additional security with firewalls or other security devices and services. This erects multiple barriers that reduce the risk of data being breached.

Think of a medieval castle, where this concept of defense in depth was an effective way to defend what was important. A moat, high thick walls, drawbridges and other chokepoints could more easily be defended due to the multiple layers of security. When entering the corporate castle today we are required to sign the visitors book or electronically complete a form to gain access. This records our visit should there be an emergency or if at a later date it is needed to prove we were there, for purposes good or bad. Monitoring who accesses or attempts to access the network, services and data enables administrators to see any suspicious behavior, then take the necessary preventive or remedial action to stop intruders from damaging or stealing the digital assets.

9. Secure remote access to your network

High speed broadband connectivity and a modern work ethic give many employees the option to work from home. For millennials this will likely become the normal modus operandi.

Any device connecting from a remote location, whether used by an employee or a client, should be subject to a security policy which requires at least the following:

- Devices not owned or controlled by the company to meet the minimum requirements of the company's hardware policy
- Connection over a Virtual Private Network (VPN)
- Strong authentication using two-factor authentication, either at the time of login or when opening a VPN connection
- Access by providing a virtualized machine as the default connection option if possible
- Anti-malware software installed and up-to-date

While we emphasize that remote devices must have active anti-malware software, it goes without saying that endpoint protection should be in place across all of your endpoints, servers and mobile devices.

10. Apply sound security practices when developing new products

Imagine the scenario where consumer data is being encrypted on servers and requires strong authentication to access it on the company network, but it is being collected from a device that does not require a password or is not using encryption to send the data. In the excitement to release a new product or service, security can often be overlooked or become an afterthought.

Make sure that your customer-facing services and products deliver a secure experience. In many cases you will be collecting personally identifiable information. Ensure that developers adopt a "secure by design" ethic from the very early stages of product development, and test products and services to ensure the security of the devices and data they're collecting. There are expert organizations that will carry out stringent tests and produce reports to show the products perform in the way they should, securely.

11. Make sure your service providers implement reasonable security measures

Web technologies have simplified connectivity between organizations, opening new opportunities for suppliers and business partners and facilitating business between companies. All too often, news stories of a data breach detail that a smaller, more vulnerable company was the conduit used by cybercriminals to access a larger and more valuable corporation.

Any service contract or agreement should include detailed requirements to ensure the third party system does not become the weakest point in your armor. Many cloud service providers go through regular penetration tests and adhere to industry standards so that you can use their services with confidence. But if you assume a large service provider has good security and practices, that won't be an adequate excuse if your customer data becomes compromised and it's found that you did not stipulate the security required or ask questions to ensure the level of security matched your own requirements. Any service provider should have policies in place that match or go beyond your own.

12. Put procedures in place to keep your security current and address vulnerabilities that may arise

"You need to patch." Security experts often say that, and with good reason. Software and hardware vendors continually create updates that fix known security issues. In recent years security patches have been made available but are not always installed. The patch to protect against the EternalBlue exploit, used to launch the WannaCry ransomware outbreak, was released 60 days before the attack.

In today's environment, it's important not only to patch, but to test for vulnerabilities. Many consumer-facing products use cloud infrastructure to deliver a service, so it's important to test infrastructure, products and services on a regular basis. Internal teams can test to a certain level and on a periodic basis, but it is also advisable to have external penetration testing carried out frequently. Expert penetration testing organizations carry out stringent tests, and produce detailed reports to show that at the time of testing, the environment was secure.

Your company can be judged by how you deal with identified vulnerabilities. Put a policy in place for handling them. It's essential both for communication and fixing the issues. A policy demonstrates a commitment to delivering a secure product that customers can trust. Most importantly, it shows a regulator or legal process that you take the security of your products and services seriously.

13. Ensure you can back up and recover data

All information technology professionals convey the importance of backups and the ability to restore from a backup. Over recent years, the incidents of ransomware malware have heightened the requirement to not only create backups, but to store them disconnected from any company system so that the infection remains isolated.

In Europe, the GDPR mandates the ability to restore availability and access to personal data in a timely manner, as well as a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures. As with many of the other recommendations, it is important to put a written process in place. It demonstrates that your organization is serious about backing up data securely and testing the recovery mechanisms frequently.

14. Promote awareness and training

Training creates awareness and a level of understanding throughout the organization. The need is at multiple levels including the compliance team, the person responsible for data and its protection, the teams that process data, the web teams that develop systems to collect data, and many more.

The data protection officer or equivalent should have a training plan in place to ensure your teams understand legislation changes and industry best practices and adhere to them. The teams that are responsible for processing data need to understand the operational requirements to be compliant with policies, regulations and legislation. Awareness of the need to protect consumer data should exist companywide, including both data protection and cybersecurity awareness. Recent data breaches show that malicious actors attempt access through the company's weakest point, and often it's the employees. Data breaches frequently start with a spear-phishing attack aimed at socially engineering an executive or an employee to give up their login credentials. Some attacks are sophisticated and look incredibly legitimate.

A starting point for a comprehensive awareness program should contain the following:

- Commitment by the executive management team that the company adheres to data protection principles and takes security seriously. This is both an internal and external message.
- Focused role based training for those that process data or have a function that uses or collects the data, including marketing, sales, call centers, and others.
- Mandatory online training cybersecurity and data protection training for all hands, on an annual or more frequent basis.
- An internal campaign to raise awareness of security and data protection principles.

15. Secure paper, physical media and devices

The technical aspects of cybersecurity can consume so much attention that it's easy to overlook the obvious. All of the previous suggestions could become irrelevant if you leave the castle door open or store the crown jewels on a table outside the walls. Any policy that covers the security of the systems that hold personal data that is covered by CCPA needs to account for physical security, too. These include secure ingress and egress to areas affording access to systems that house personally identifiable data, keeping laptops and external drives secure from theft, and shredding documents that contain information covered by the CCPA.

How ESET can help

ESET offers a number of solutions that work together to help you bolster your cybersecurity, and achieve and demonstrate "reasonable security" in support of your CCPA compliance efforts.

Endpoint Protection

Comprehensive multilayered security combining machine learning and human expertise

- Balances performance, detection and false positives
- Enables organizations to prevent data breaches, protect against ransomware, block targeted attacks, stop fileless attacks and detect APTs
- Blocks network-level vulnerabilities that can spread malware

Endpoint Encryption

Easy-to-use encryption application with fast, seamless deployment and zero impact on productivity

- Provides full remote control of endpoint encryption keys; manage devices from anywhere
- Enforces security policy for files on hard drives, portable devices and emails
- Protects sensitive data by means of full-disk encryption (FDE)

Multi-Factor Authentication

One-tap mobile-based authentication for data protection

- Provides simple, effective way for businesses of all sizes to implement multi-factor authentication
- Enables your organization to prevent data breaches, easily manage authentication and secure mobile devices

Cybersecurity Awareness Training

Free, simple and on demand cybersecurity awareness training

- Keep employees focused with interactive training
- Lower your risk with training that truly changes behavior
- Document your training initiative with ESET's certification

Data Loss Prevention

Protection from Safetica against expensive data leaks and unnecessary personnel costs

- Covers all data leak channels
- Saves the cost of repairing a data breach
- Identifies suspicious activities before they result in lost time and money
- Reduces personnel costs by identifying productivity issues and improving work

Backup and Recovery

Comprehensive backup and recovery from Xopero Software

- Protects your business data no matter where it is stored
- Covers your entire environment, from endpoints to Microsoft Exchange to virtual environments

Conclusion

To protect your business, it's important to get started on your CCPA compliance efforts now. First, find out if you're subject to the act. If you are, start to get your data house in order with respect to how you handle personal information. Equally important, take the security aspect seriously. The high penalties related to data breaches are a huge business risk, making compliance a must no matter your size.

To learn more about CCPA, how it may impact your current cybersecurity profile and what steps to take next, or to explore ESET solutions, visit: eset.com/us/ccpa

Disclaimer

This paper is a general overview of the CCPA only, and is not intended as legal advice. The overview reflects the act as understood as of the date of publication. For legal advice and your compliance, contact a qualified attorney.