Live Webinar | GDPR vs. CCPA vs. CCPA 2.0: 10 Critical Differences

Presented by

Scott M. Giordano

Esq., FIP, CISSP, VP and Sr. Counsel, Privacy and Compliance

Spirion

ISMG INFORMATION SECURITY MEDIA GROUP

SPIRION

About Information Security Media Group

- Focused on providing information security content, specifically for unique vertical industries
- Publish articles, interviews, blogs, regulation & guidance alerts, and whitepapers
- Educational webinars offered daily

BANK INFO SECURITY®

CU INFO SECURITY® Just for Credit Unions

GOV INFO SECURITY®

HEALTHCARE INFO SECURITY®

Data Breach TODAY
Prevention. Response. Notification.

CAREERS INFO SECURITY®

infoRisk TODAY®

Technical Support

(609) 356-1499 x115

About Sponsor

Spirion is a pioneer in designing the critical first step of data security and privacy through its data discovery, persistent classification, and behavior software and services. The company was recently ranked by CIOReview magazine as one of the “20 Most Promising Compliance Technology Solution Providers of 2019,” an annual listing of 20 companies that are at the forefront of providing compliance technology solutions and transforming businesses. Spirion is an award-winning data privacy software company with recent wins in the Info Security Products Guide 2020 Global Excellence Awards as a Grand Trophy Winner and as a winner in specific categories for SaaS, cloud, and on-premise data discovery and classification. For more information, visit spirion.com.

About the Speaker

Scott M. Giordano

Esq., FIP, CISSP, VP and Sr. Counsel, Privacy and Compliance, Spirion

Scott M. Giordano is an attorney with more than 20 years of legal, technology, and risk management consulting experience. An IAPP Fellow of Information Privacy and a Certified Information Security Systems Professional (CISSP), Scott serves as Spirion's subject matter expert on multinational data protection and its intersection with technology, export compliance, internal investigations, information governance, and risk management. During his career, Scott has held senior positions at several legal technology firms and is listed as co-inventor on Intelligent Searching of Electronically Stored Information, patent application no. 13/842,910. In addition, he taught the first law school course anywhere on electronic evidence and e-discovery. Scott is a member of the bar in Washington state, California, and the District of Columbia.

GDPR vs. CCPA vs. CCPA 2.0: 10 Critical Differences

Scott M. Giordano, Esq., FIP, CISSP
V.P. and Sr. Counsel, Privacy and Compliance
Scott.Giordano@Spirion.com

April 14, 2020

If you leave with nothing else…

- CCPA enforcement date is still July 1, 2020; CCPA lawsuits continue to roll in
- CCPA 2.0 status seems to be on track in spite of the lockdown
- GDPR enforcement had been strong in 2020 until now
- Being compliant with one regime does not mean compliance with another
- Beware of non-financial penalties
- There's a lot more than we can cover today

SPIRION

Jurisdictional Scope

Jurisdictional Scope

	GDPR	CCPA	CCPA 2.0
Applies to:	Businesses, Government Bodies, Non-Profits	Businesses	Businesses
Who is regulated?	Any organization (known as data controllers and data processors) that is: A. Established in the EU; or Is outside the EU but A. Offers goods or services in the EU; or B. Monitors or tracks the behavior of EU data subjects within the EU	Any for-profit entity doing business in California and A. Has annual gross revenues in excess of $25 million; or B. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or C. Derives 50% or more of its annual revenues from selling consumers' personal	Any for-profit entity doing business in California and A. Had gross revenue greater than $25 million in the preceding year; or B. Alone or in combination, annually buys or sells the personal information of 100,000 or more consumers or households C. Derives 50% or more of annual revenue from selling consumers' personal information

Jurisdictional Scope - Summary

- All three laws have potentially global application
- “Offering goods or services” into the EU can be a complex calculation
- We still don’t know if the CCPA $25M threshold is within California or global, so assume California for now
- CCPA applies to for-profit healthcare and higher education
- CCPA 2.0 has a potentially higher jurisdictional threshold
- Note the “common branding” issue of CCPA – applies to entities that share the brand (typically parent companies); CCPA 2.0 adds “and with whom the business shares consumers’ personal information.”

SPIRION

Controllers/ Businesses vs. Processors/Service Providers

Controllers/Businesses vs. Processors/Service Providers

	GDPR	CCPA	CCPA 2.0
Entity Name and Definition	• **Controller.** An entity which, alone or jointly with others, determines the purposes and means of the processing of personal data • **Processor.** An entity which processes personal data on behalf of the controller	• **Business.** A for-profit entity that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information • **Service Provider.** An entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract	• **Business.** A for-profit entity that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information. • **Service Provider.** A person that processes personal information on behalf of a business and which receives from or on behalf of the business a consumer's personal information for a business purpose pursuant to a written contract • **Contractor.** A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract
Applicable Portion of the Regulation or Act	• **Controller.** All of the GDPR, primarily Chapters 1-5 • **Processor.** Primarily most of Chapter 4, and in particular, Art. 28	• **Business.** All of the CCPA • **Service Provider.** Limited CCPA applicability; e.g., §105(c) regarding deletion of personal information; Indirectly, those CCPA provisions that define a business's relationship with the provider, e.g., §140(t)(2)(C)(ii)	• **Business.** All of the CCPA • **Service Provider.** Limited CCPA applicability; e.g., §105(c) regarding deletion of personal information; Indirectly, those CCPA provisions that define a business's relationship with the provider, e.g., §140(t)(2)(C)(ii) • **Contractor.** Must notify the business of sub-contractors and flow down contractual restrictions

Controllers/Businesses vs. Processors/Service Providers - Summary

- Controller vs. Processor relationship clearly defined in the GDPR, with Art. 28 being primary for Processors; regulation of sub-processor relationships outside of the EU can get a bit murky
- CCPA is mostly “hands off” with respect to regulation of Service Providers – at least for now
- CCPA 2.0 acknowledges by name the idea of a Contractor, (which the CCPA merely implies) and mandates imposition of its own terms on sub-Contractors

SPIRION

Personal Data vs. Personal Information

Personal Data vs. Personal Information

	GDPR	CCPA	CCPA 2.0
Principle Definition	• Personal data. Any information relating to an identified or identifiable natural person (‘data subject’)[.]	• Personal information. Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	• Personal information. information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
Secondary Definition	• an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier • or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[]	• Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[]	• Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household[]

Personal Data vs. Personal Information

	GDPR	CCPA	CCPA 2.0
Machine-readable data	• [O]nline identifiers provided by… devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.	Any of the examples cited in §140(o)(1)(A)-(K) that are in electronic form fall into this category, such as: • Social Security numbers • Purchase histories • Biometric information • Internet search history • Geolocation data • Professional/employment information • Education information • Consumer profiles	Any of the examples cited in §140(o)(1)(A)-(K) that are in electronic form fall into this category, such as: • Social Security numbers • Purchase histories • Biometric information • Internet search history • Geolocation data • Professional/employment information • Education information • Consumer profiles
Special or Sensitive Personal Data	Special Personal Data • [P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, • The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, • Data concerning health or data concerning a natural person's sex life or sexual orientation	The CCPA does not identify any personal data as "special" or "sensitive." Note that personal data as defined by HIPAA or its California analog, the Confidentiality of Medical Information Act (CMIA), is excluded from the scope of the CCPA	Sensitive personal information. • A consumer's social security, driver's license, state identification card, or passport number; • A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; • A consumer's precise geolocation; • Personal information revealing a consumer's racial or ethnic origin, religion, or union membership; • The contents of a consumer's private communications, unless the business is the intended recipient of the communication; • A consumer's biometric information; • Data concerning a consumer's health; • Data concerning a consumer's sexual orientation; or

Personal Data vs. Personal Information - Summary

- All three regimes include the “directly or indirectly” qualifier, making the threshold for being “identifiable” very low
- CCPA 2.0 sensitive personal information restricts use, not just sale

SPIRION

Legal Basis vs. Consent

Legal Basis vs. Consent

	GDPR	CCPA	CCPA 2.0
Principle Definition	Art. 6: • Consent • Contract • EU legal obligation • Vital interest of an individual • Public interest • Legitimate interest Art. 9(2): • Consent • Employment and social security • Vital interests of an individual • Legitimate interest of a non-profit for its members • Publicly available • Legal defense • Public health • Archiving public interest, scientific, or historical research	• CCPA Text. No per se legal basis required; consumers have the right to opt out of sale of personal information to third parties • Mandates that businesses that wish to collect the personal data of children are required to obtain consent to sale of their personal data; children 13-16 can provide direct consent while children under 13 require parental consent • CCPA Regulations. "If the business intends seeks to use a consumer's previously collected personal information for a purpose that materially different than what was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose."	• CCPA 2.0 Text. No per se legal basis required; consumers have the right to opt out of sale of "regular" personal information to third parties • Consumers must opt in for use of sensitive personal information by businesses or sale to third parties • Prohibits businesses from collecting the personal information of children under 16 unless the child (if 13 or older) or parent has affirmatively consented to the collection (i.e., opted in)

Legal Basis vs. Consent - Summary

- GPDR requires a true legal basis; not (yet) so with CCPA
- Legitimate interest requires a legitimate interest analysis (LIA) for validity
- Under GDPR, cross-border data transfers require their own legal basis

SPIRION

Right to Erasure vs. Deletion

Right to Erasure vs. Deletion

	GDPR	CCPA	CCPA 2.0
Principle Definition	Art. 17. "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." Exceptions: • The controller has a need for the personal data • There is another legal ground for processing if consent is withdrawn • There are overriding legitimate grounds even in the face of objection by the data subject The Right to Erasure applies to all personal data, not just that data collected from the data subject Limitations. The following may also limit the application of the Right to Erasure: • Freedom of expression • Compliance with an EU legal obligation or public interest processing • Public health • Archiving for public interest, scientific or historical research purposes	Sec. 105. A consumer may request that personal information "that the business has collected from the consumer" be deleted. The business shall delete the consumer's personal information from its records, and direct any service providers to delete the consumer's personal information from their records. Exceptions: • Complete a transaction or fulfill a warranty • Information security • Debug or repair error • Free speech • Comply with the California Electronic Communications Privacy Act (ECPA) • Research in the public interest • Solely internal uses • Comply with a legal obligation • Compatible with the context in which the consumer provided the information The right to deletion applies only to data collected from the consumer	Sec. 105. A consumer may request that personal information "that the business has collected from the consumer" be deleted. The business shall delete the consumer's personal information from its records, and direct any service providers or contractors to delete the consumer's personal information from their records, and direct all third parties who have accessed such personal information from or through the business to delete the consumer's personal information. Exceptions: • Complete a transaction or fulfill a warranty • Information security • Debug or repair error • Free speech • Comply with the California ECPA • Research in the public interest • Solely internal uses • Comply with a legal obligation • Compatible with the context in which the consumer provided the information Note that contractors can claim these exceptions The right to deletion applies only to data collected from the consumer

Right to Erasure vs. Deletion

	GDPR	CCPA	CCPA 2.0
Time limit	**Art. 17.** "[W]ithout undue delay." Generally speaking, the time limit for deletion is one month. Extensions of time are available in extreme circumstances	**Secs. 105 and 130(a)(2).** "[W]ithin 45 days of receiving a verifiable consumer request from the consumer." May extend for up to 90 days, but must notify consumer within the 45-day window and provide a reason for the delay Note: Per **§105**, the Business must direct any service providers to delete the consumer's personal information from their records. Per **§999.313(a)** of the draft CCPA Regulations, must acknowledge the consumer's request within 10 business days of receipt and delete within 45 calendar	**Secs. 105 and 130(a)(2)(A).** "[W]ithin 45 days of receiving a verifiable consumer request from the consumer." Note: Per **§105**, the Business must direct any service providers, contractors, and third parties to delete the consumer's personal information from their records.

Right to Erasure vs. Deletion - Summary

- There are no absolute rights to erasure/deletion – each has exceptions and limits
- CCPA version only applies to data collected from the consumer; this could be significant
- CCPA requires businesses to direct service providers to delete as well; CCPA 2.0 includes contractors and third parties
- Also note that California has a “Right to be Forgotten” for minors, which allows erasure of their content from websites or mobile applications
- Legal counsel should be involved throughout this process; there are many ways this can go wrong

SPIRION

Sales of Data to Third Parties

Sales of Data to Third Parties

	GDPR	CCPA	CCPA 2.0
Principle Definitions	Sale. The GDPR does not define a "sale" of personal data. In fact, the word "sale" does not appear in the GDPR. Third party. An entity other than the data subject, controller, or processor, is under the direct authority of the controller or processor, and is authorized to process personal data. Onward transfer. The GDPR describes (but does not define) the concept of an "onward transfer" in Rec. 101, which is a transfer of personal data outside of the EU. The requirements for onward transfers cited in Arts. 44-50 must be met, in addition to threshold matters such as legal basis and purpose limitation.	Sale. Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. Third Party. Per §140(w), a third party is a recipient of personal information who is <u>not</u> the business that collected it nor an entity operating on behalf of that business based on a contract	Sale. Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose, including but not limited to cross-context behavioral advertising. Third Party. Per §140(ah), a third party is <u>not</u> the following: • The business that collected the personal data; or • A service provider to the business; or • A contractor

Sales of Data to Third Parties

	GDPR	CCPA	CCPA 2.0
Rules Governing Sale/ Transfer	Under GDPR, there are no per se prohibitions for sales or transfer of person data to third parties, assuming there is a valid legal basis for processing that data in the first place and there are no changes that would vitiate that basis (e.g., using the data for different purpose that consented to by the data subject). Art. 5(1)(b) articulates this idea under the principle of "purpose limitation," i.e., no processing that is out of scope of what was initially contemplated when the personal data was collected. Controller-to-Controller and Controller-to-Processor transfers require an underlying Data Processing Agreement (or DPA). The terms of the DPA must be flowed down to sub-processors. Transfers of personal data outside of the EU require their own legal basis, such as the use of Standard Contract Clauses.	• Sec. 120(a). A consumer can direct a business not to sell the consumer's personal information. • Sec. 120(b). A business that shall provide notice to consumers that their personal information may be sold to third parties and that consumers have the right to opt out. • Sec. 115(d). A third party shall not sell personal information about a consumer unless the consumer has received explicit notice and is provided an opportunity to opt out.	• Sec. 120(a). A consumer can direct a business not to sell the consumer's personal information. • Sec. 120(b). A business that shall provide notice to consumers that their personal information may be sold to third parties and that consumers have the right to opt out. • Sec. 120(c). A consumer can direct a business not to use the consumer's sensitive personal information for advertising or marketing, nor to disclose it to a service provider or contractor. • Sec. 115(d). A third party shall not sell personal information about a consumer unless the consumer has received explicit notice and is provided an opportunity to opt out.

Sales of Data to Third Parties - Summary

- The GDPR does not define a “sale,” but note legal basis and Art. 5 “purpose limitation”
- Threshold for a “sale” under CCPA is very low
- Beware the “service provider” loophole
- Current state of Do Not Track under the CCPA Regulations:
  - “If a business collects personal information from consumers online, the **business shall treat user-enabled global privacy controls**, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to **opt-out of the sale of their personal information as a valid request [to opt out of such a sale]**…**for the consumer**[.]”

SPIRION

SPIRION

Right to Object

Right to Object

	GDPR	CCPA	CCPA 2.0
Principle Definitions	Art. 21. Data subjects have the right to object to processing if the underlying legal basis is Arts. 6(1)(e) (public interest) or (f) (legitimate interest). The data controller then has to have "compelling legitimate grounds" to continue processing. In the case of "information society services," the data subject must be able to "object by automated means" (presumably a web browser).	There is no per se right to object to processing under the CCPA. The closest analog is the right to opt out of sales of personal information under §§120(a) and (b) and under §115(d).	There is no per se right to object to processing under CCPA 2.0. The closest analog is the right to opt out of sales of personal information under §§120(a), (b), and (c) and under §115(d).

Right to Object

- RTO is unique to the GDPR, and is periodically cited in GDPR-related investigations by supervisory authorities (e.g., the Garante's recent investigations and fines against TIM SpA and ENI Gas e Luce).
- Notes on "information society services" per the U.K. Information Commissioners Office (ICO):
  - It generally includes websites, apps, search engines, online marketplaces and online content services such as on-demand music, gaming and video services and downloads.
  - It does not include traditional television or radio transmissions that are provided via general broadcast rather than at the request of an individual.

Opting Out of Marketing and Advertising

SPIRION

Opting Out of Marketing and Advertising

	GDPR	CCPA	CCPA 2.0
Principle Definitions	• Art. 21(2). Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing, which includes profiling. • Art. 21(3). Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. • Art. 21(4). At the latest at the time of the first communication with the data subject, the right referred to [above] shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	There is no per se right to opt out of advertising or marketing under the CCPA. However, the right to opt out of sales of personal information under §§120(a) and (b) and under §115(d) effectively creates an opt out.	Under CCPA 2.0, the concept of "advertising and marketing" is defined and regulated. Under §120(c), "A consumer shall have the right, at any time, to direct a business that uses or discloses sensitive personal information about the consumer for advertising and marketing not to use the consumer's sensitive personal information or disclose it to a service provider or contractor, for advertising and marketing." "A business that uses or discloses a consumer's sensitive personal information for advertising and marketing shall provide notice to consumers…that consumers have the 'right to opt-out'"

Opting Out of Marketing and Advertising - Summary

- Under GDPR Art. 21(3), the right to opt out of marketing is absolute
- Note that under Art. 21(4), as the data controller, these rights "shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information."

Children’s Data

Children's Data

	GDPR	CCPA	CCPA 2.0
Principle Definitions	Art. 8. When the processing of a child's personal data is based on consent, the child must be at least 16 years old. Otherwise, a parent must give the consent. EU member states can lower this age threshold down to the age of 13.	Sec. 120. If a business has actual knowledge that a consumer is younger than 16 years of age, it can not sell that consumer's data, unless: • The consumer has consented, in the case of a consumer at least 13 years of age; or • The child's parent consent, for children younger than 13 This is known as "right to opt-in." A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.	Sec. 100(g)(1). If a business has actual knowledge that a consumer is younger than 16 years of age, it cannot sell that consumer's data, unless: • The consumer has consented, in the case of a consumer at least 13 years of age; or • The child's parent consent, for children younger than 13 This is known as "right to opt- in." A business that willfully disregards the consumer's age or that has actual knowledge per the Children's Online Privacy Protection Act (COPPA) shall be deemed to have had actual knowledge of the consumer's age. If the consumer, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, declines to affirmatively authorize the collection of the consumer's personal information … the business shall refrain from collecting the consumer's personal information and shall wait for at least 12 months before requesting the consumer's consent again.

Children's Data - Summary

- Processing children's data under CCPA is based on "opt-in" consent
- Note the updated CCPA 2.0 constructive knowledge standard:
  - A business that willfully disregards the consumer's age, or that has actual knowledge, as that term is used in regulations implementing the Children's Online Privacy Protection Act, 15 U.S.C. section 6501, et. seq., of the consumer's age, shall be deemed to have had actual knowledge of the consumer's age.

Data Subject Access Requests/ Consumer Data Access Requests

SPIRION

Data Subject Access Requests/Consumer Data Access Requests

	GDPR	CCPA	CCPA 2.0
Principle Definitions	Art. 15. The data subject shall have the right to obtain from the controller confirmation …access to [their] personal data and the following information: a) the purposes of the processing; b) the categories of personal data processed; c) the recipients or categories of recipient…in particular recipients in third countries or international organizations; d) where possible, the envisaged period for which the personal data will be stored; e) the right to request rectification, erasure, restriction of processing, or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) if the personal data wasn't collected from the data subject, any available information as to the source; h) the existence of automated decision-making Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.	Sec. 110(a). The Big 5 areas of personal information that businesses must disclose to consumers: • [What] the categories of personal information it has collected about that consumer; • [Where] the categories of sources from which the personal information is collected; • [Why] the business or commercial purpose for collecting or selling personal information; • [Who] the categories of third parties with whom the business shares personal information; and • [What] the specific pieces of personal information it has collected about that consumer. They show up throughout the CCPA, directly and indirectly: §§ 100, 110, 115.	Sec. 110(a). The Big 6 areas of personal information that businesses must disclose to consumers: • [What] the categories of personal information it has collected about that consumer; • [Where] the categories of sources from which the personal information is collected; • [Why] the business or commercial purpose for collecting or selling personal information; • [Who] the categories of third parties with whom the business shares personal information; • [Why] political uses of the personal information; and • [What] the specific pieces of personal information it has collected about that consumer. They show up throughout the CCPA, directly and indirectly: §§ 100, 110, 115.

Data Subject Access Requests/Consumer Data Access Requests

	GDPR	CCPA	CCPA 2.0
Time Limits and Production Format	Art. 12. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Art. 15. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	Sec. 130. Businesses have 45 days to complete a request by a California consumer to disclose and deliver a copy of the personal information that the business has collected. The business can extend this period by an additional 45-day period. The scope of the personal information is limited to that which was collected in the preceding 12-month period. Sec. 999.313 of the CCPA Regulations: • Acknowledgement. Businesses have 10 business days to respond to a "Request to Know" by a consumer. • Fulfillment. Businesses have 45 calendar days from the time the Request to Know is received to complete its fulfillment. They can extend by 90 additional days if they notify the requestor and cite the reason for the delay. The information must be "in a form that is reasonably accessible to consumers."	Sec. 130. Businesses have 45 days to complete a request by a California consumer to disclose and deliver a copy of the personal information that the business has collected. The business can extend this period by an additional 45-day period. The information must be "in a form that is reasonably accessible to consumers."

Data Subject Access Requests/ Consumer Data Access Requests - Summary

- DSARs/CDARs likely the respective areas of each law that produce the most questions.
- This is arguably the entire basis for your data inventory
- Note the unique requirement under CCPA 2.0 to provide, as part of Sec. 110 disclosures, uses of personal information for political purposes:
  - **If the business uses personal information it has collected about consumers for political purposes on its own behalf**, the name or names of the candidate or candidates, committee or committees, and/or the title or titles of the ballot measure or measures for which consumers' personal information was used for political purposes, and whether the consumers' personal information was used to support or oppose the candidate, committee, or measure.

Summary and Conclusions

Summary and Conclusions

- Most common Arts. Cited in GDPR investigations: 5, 6; 32
- Most implied: 17, 21
- No published implementation or audit guidelines from EDPB, nor is any on the horizon
  - There are guides for some Articles: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
- At this point, about four lawsuits related to CCPA; expect more to follow
- We are on our second revision of the CCPA Regulations; additional ones are entirely possible

Summary and Conclusions

- NIST Privacy Framework perhaps the best place to start
- ISO 27701 Privacy Information Management System (PIMS) has some potential
- Security standards, guidelines, and frameworks such as ISO/IEC 27001/2, NIST 800-171, and CSC Top 20 can address Art. 32 and, indirectly, other articles that cite “technical and organizational” requirements
- Business partners (vendors, third parties, licensees, etc.) require vigorous policing
- Time for a Privacy Operations Center?
- **Understanding where personal information is located within your organization and who has access to it will be key to advancing compliance**

Sample Data Inventory

Process Descriptions							
Nerve Center' Country (dropdown)	Business teams (dropdown)	Business process activity (e.g. recruiting, payroll calculations, payment processing, etc.)	Description, why activity is done (possible highlight if privacy notice or consent required)	Employees, Customers, Candidates, Suppliers (dropdown)	Types of Personal Data include name, address, date of birth, marital status	personal data type (Standard or Sensitive) - sensitive data type include standard personal data fields	Legal basis for processing
Country	Business Unit	Process flow name	Purpose of the processing	Category of Persor	List of data items	Data Type	Legal Basis
United States	IT	MDM Expert	Mobile Device Management (MDM). Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM) which also includes mobile application management, identity and access management and enterprise file sync and share. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.	Employee	IMSI, IMEI, Device ID, ESN	Standard	Legitimate Interest
United States	IT	DLP Master	Data loss prevention; specifically, file centric actions - e.g., copying from a Word document to Yahoo mail or a USB drive. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.	Employee	Equipment identifier (laptop, desktop ID or processor serial number), UserID, AD credentials	Standard	Legitimate Interest

Reproduced with permission from Robert Half Legal Consulting

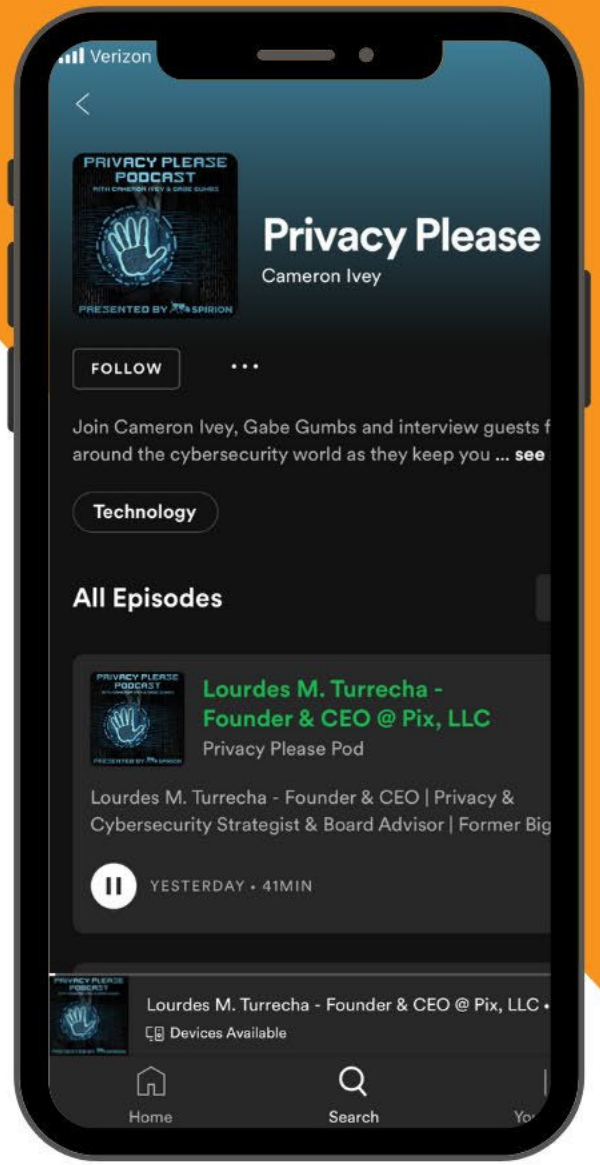
SPIRION

SPIRION

Visit Our Privacy Please Podcast

Available on Spotify, Google Podcasts, iTunes or anywhere you get your podcasts.

LISTEN NOW

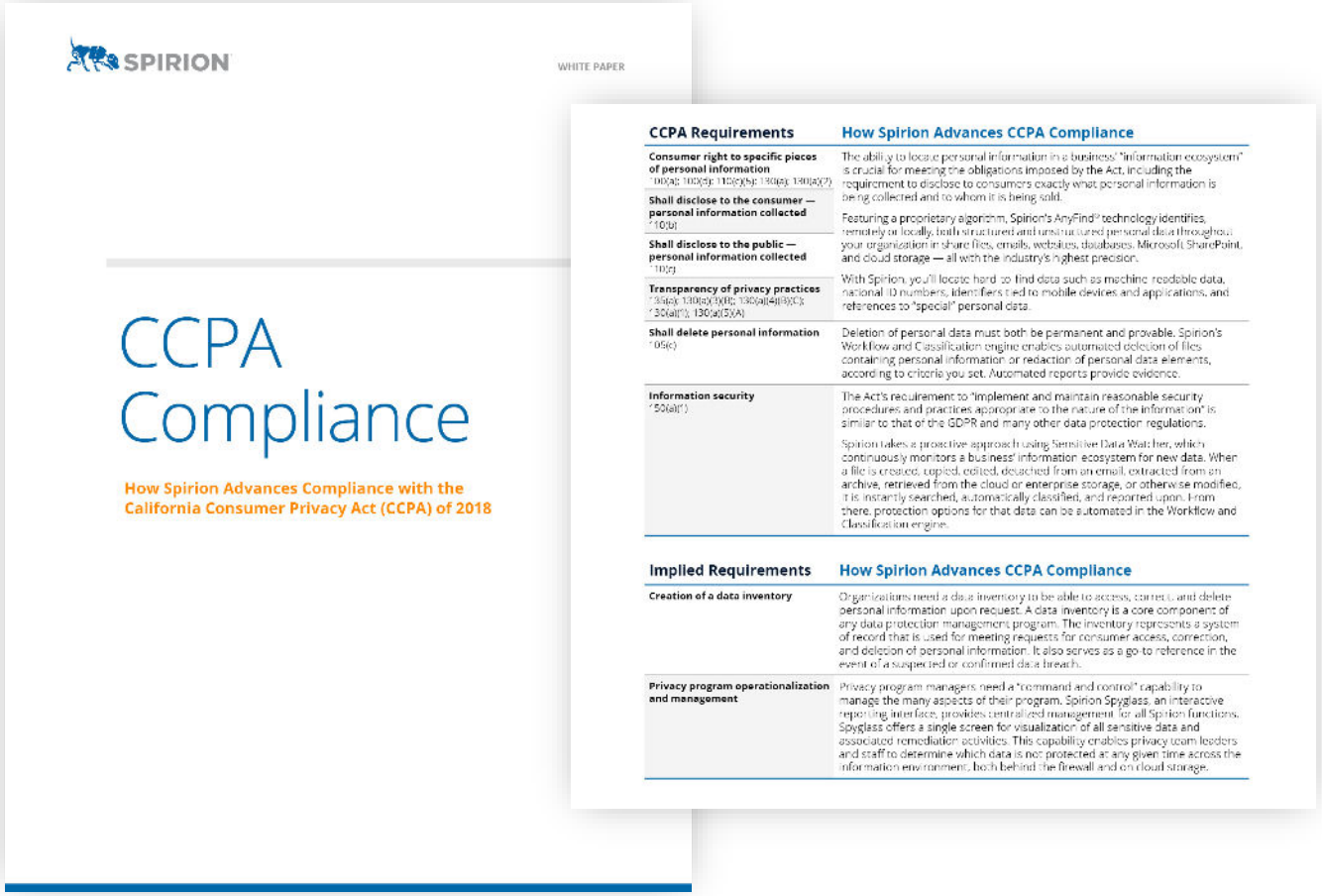


Thank you!

Scott M. Giordano, Esq.
Scott.Giordano@Spirion.com

Learn more about how Spirion can help accelerate CCPA compliance through automated accurate data discovery, classification and monitoring.

Visit www.spirion.com



Questions

Please use the following form for any questions or comments:

http://www.bankinfosecurity.com/webinar-feedback.php

Or contact us at: (800) 944-0401

Thank You for Participating!

Please use the following form for any questions or comments:

http://www.bankinfosecurity.com/webinar-feedback.php

Or contact us at: (800) 944-0401