Complying with Data Protection Regulations

Vandana Mansharamani (vandana.mansharamani@sap.com) is Product Manager – Security and Data Protection for SAP S/4HANA Cloud. Please note that she is not a lawyer, and she does not provide legal advice.

How Features in SAP S/4HANA Cloud Help Organizations Comply with GDPR and CCPA

Regulatory compliance is a big deal, and not just because it can require a huge amount of resources and effort to ensure that your organization adheres to all relevant laws and regulations — it's also because violations can be even more costly. As former US Deputy Attorney General Paul McNulty is quoted as saying, "If you think compliance is expensive, try non-compliance." To avoid penalties, companies must be constantly aware and ready to adapt to new and changing requirements, and one area that is seeing a growing amount of regulation is data protection. Data protection regulations enable individuals to exercise control over their personal information, and force organizations to stop, think, and act when it comes to their data privacy practices — for example, businesses must consider the purpose of their data collection and whether their data processing practices are ethical.

One of the most wide-reaching of these data protection regulations is the European General Data Protection Regulation (GDPR), which went into full effect on May 25, 2018, replacing the existing 95/46/EC data protection directive with a wider scope and increased penalties for non-compliance. GDPR protects the personal data of individuals residing within the European Union (EU) and applies to any company that processes data, offers services or goods, or monitors the behavior of people in the EU, regardless of whether that company is physically located in the EU.

Since this regulation went into effect, countries around the globe have continued to adopt data protection laws. In the US, for example, the state of California has added the California Consumer Privacy Act (CCPA) of 2018,[1]

[1] Learn more at http://bit.ly/CAConsumerPrivacyAct.

which takes effect on January 1, 2020. CCPA applies to organizations that do business in the state of California, whether they are physically located in California or elsewhere. With California's economy among the largest in the world,[2] CCPA has consequences for businesses across the globe.

A previous SAPinsider article[3] took a detailed look at GDPR and how SAP Business Suite solutions help businesses comply with this regulation. This article builds on the previous one by looking at the additional effects of the new CCPA regulation, and how features embedded in SAP S/4HANA Cloud help SAP customers address both CCPA and GDPR requirements.[4]

What Is CCPA?

Under CCPA, consumers — defined as California residents who have been identified in some way by a business that is located either within California or elsewhere — have the right to safeguard their privacy and have control over personal information that is collected and used in some way by a business that meets at least one of the following criteria:

- Has an annual gross revenue greater than $25 million
- Processes the personal information of 50,000 or more consumers, households, or devices
- Derives 50% or more of its annual revenue from selling consumers' personal information

So, what types of information does this legislation cover, and what kind of control do consumers have? Let's take a closer look at what qualifies as personal information according to CCPA, and the specific rights that consumers have regarding this information.[5]

How Does CCPA Define "Personal Information"?

The CCPA definition of personal information is expansive — it encompasses any information that identifies, relates to, describes, is capable of being associated with, and could reasonably be linked directly or indirectly with a particular consumer or household.

Examples include traditional identifiers such as name, postal or email address, and social security number; online identifiers such as account name and IP address; categories of personal information and classifications protected by law, such as race and sexual orientation; behavioral information, such as purchasing history, online browsing or search history, and website or advertisement interactions; biometric, geolocation, and sensory data; professional and educational information; and consumer profiles built from any of this personal information.

Note that personal information as defined by CCPA does not include information that federal, state, and local governments lawfully make publicly available. However, if that data is used by a business for a purpose other than that for which it was made available, then it is not considered publicly available information under CCPA.

How Does CCPA Define Consumer Rights?

Under CCPA, businesses must honor verifiable requests from consumers regarding the use of their personal information. CCPA defines the following six consumer rights — the first five explicitly and the sixth implicitly — regarding the use of this information:

- **Right 1 (Section 1798.100): What personal information about me do you have?** Upon a consumer's request, the business must share with the consumer the categories and specific pieces of personal information that were collected within the last 12 months.
- **Right 2 (Section 1798.105): You will delete my data upon my request.** Upon a consumer's request, a business must delete a consumer's personal information unless there is a valid or legal reason to deny that request.
- **Right 3 (Section 1798.110): What personal information about me do you have from**

[2] https://www.bloomberg.com/opinion/articles/2019-04-24/california-economy-soars-above-u-k-france-and-italy

[3] See the SAPinsider article "Meeting Modern Data Protection Requirements" (Issue 3 2017) available at SAPinsiderOnline.com.

[4] Note that the author of this article is not a lawyer by profession, and that this article is not intended to provide legal advice.

[5] For full details on any portions of the CCPA legislation discussed in this article, see http://bit.ly/CAConsumerPrivacyAct.

other sources, why do you have it, and where did you get it? Upon a consumer's request, if the business collects data about the consumer from other sources, it must disclose the categories of personal information collected, the sources from which it was collected, why it was collected, and why and with whom it was shared. The business must also disclose the specific pieces of personal information that were collected.

- **Right 4 (Section 1798.115): Are you selling or disclosing my data, and if so, what data, why, and to whom?** Upon a consumer's request, the business must divulge the categories of personal information it collected about that consumer, the categories of personal information it sold or disclosed, and the categories of third parties to which it was sold or disclosed, including which category of data to which particular third party. Additionally, if the business both sells and discloses personal information, it must provide two separate reports with the relevant information. Distinguishing between the sale and disclosure of personal information helps to avoid any confusion around what constitutes the "sharing" of data.

- **Right 5 (Section 1798.120): I have the right to opt out of the sale of my personal data.** A business that sells personal information must let consumers know in advance that their data may be sold, and the business must provide a conspicuous link on its website that enables consumers to opt out of the sale of their information. In addition, businesses are prohibited from selling the personal information of consumers less than 16 years of age without authorized consent — for consumers under the age of 13, consent from a parent or guardian is required; consumers aged 13-16 must give their own consent.

- **Right 6 (Section 1798.125): You will not discriminate against me if I exercise my rights.** A business is prohibited from discriminating against consumers who exercise their rights by denying goods and services, charging a different price, or providing a lower quality version of the product or service. An exception would be if the lack of data prevents the business from offering the product or service — if a consumer's home address is withheld from a service company hired to repair the consumer's dishwasher, for example.

Under CCPA, a consumer can choose to exercise any of these rights with businesses that collect, use, and disclose their personal data.

How Do Companies Ensure Legal Compliance?

Meeting the legal obligations defined by regulations such as CCPA and GDPR can require different types of technical and organizational measures. Technical measures are actions that need to be taken in an application or a computerized system, such as SAP S/4HANA Cloud. For instance, deleting data requires delete functionality to be available in the application. Organizational measures, on the other hand, are actions that ensure the smooth and effective operation of an organization.

These two types of measures can be complementary — for example, organizational measures could be supported by technical measures. The organizational measure of requiring a badge for an employee to enter the premises would be supported by the technical measure of assigning an ID to that employee in the database and then linking the badge to this ID, for instance. The measures can also exist independently — for example, an organizational measure might require that all employees follow a clean desk policy and lock all documents before leaving the premises.

The appropriate and relevant technical and organizational measures for a business are highly specific to the company that implements them. For example, a company that implements a software solution for the military might require that all consultants working on the project have security clearance, while a company that makes software might not require security clearance but could have stringent rules around intellectual property for patents filed by their employees. It all comes down to the nature of the company. In all cases, the foundation is a comprehensive evaluation and consultation with stakeholders across the organization, including business, IT, and legal departments.

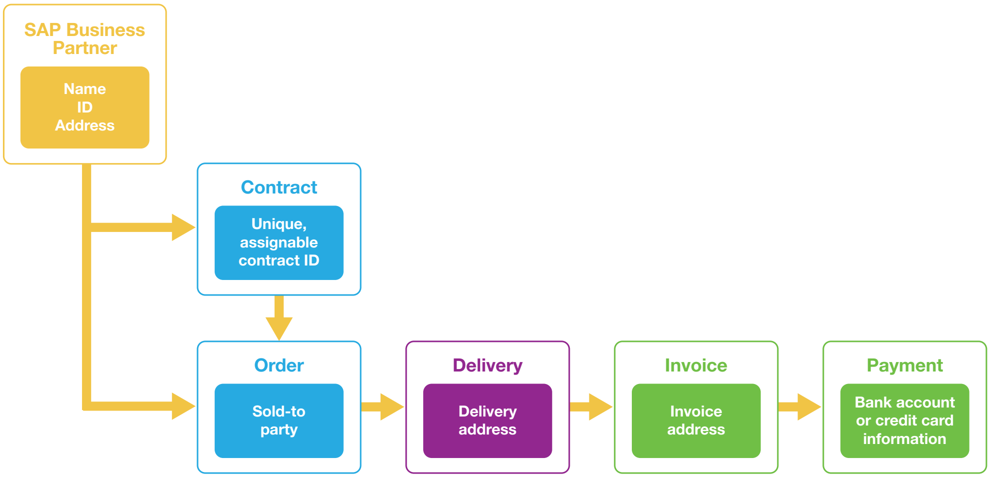

Figure 1 Examples of personal data in SAP applications such as SAP S/4HANA Cloud

How Do SAP Solutions Help with Compliance?

SAP software helps organizations run their enterprise processes, and these business processes sometimes require personal data such as business partner names, addresses, bank account numbers, and credit card numbers. **Figure 1** shows some examples of personal data that could be present in SAP applications such as SAP S/4HANA Cloud.

SAP has embedded features into SAP S/4HANA Cloud that provide the enterprises using them with a means to comply with data protection regulations such as CCPA and GDPR. These features include:

- Standard edit functionality for ensuring data accuracy
- Identity and access management features for minimizing data access
- Data management capabilities for erasing data once its purpose is complete
- An information retrieval framework for providing information to subjects about their data
- Logging and organizational modeling features for proving accountability via technical and organizational measures

Note that while these features support some of the CCPA and GDPR requirements of these laws, they do not make the product itself compliant out of the box. Using these features to meet your business and legal needs must be coordinated with your business, IT, and legal departments to ensure full compliance.

Let's take a closer look at how some of the features available with SAP S/4HANA Cloud can help with implementing data protection measures required by CCPA and GDPR. Since the standard edit functionality present in essentially all SAP applications, which supports the data accuracy requirement, is fairly straightforward, we'll focus on the other four types of features.

Minimizing Data Access

SAP S/4HANA Cloud includes a robust authorization concept to help minimize data access. Under CCPA and GDPR, access to data must be controlled according to purpose. For example, not every person in your organization should be able to see all personal information about a business partner or customer. To verify the identity of a customer calling a bank to inquire about an account, for instance, the last four digits of the customer's account number and the customer's birth date should suffice — additional information about religion or race should not be required.

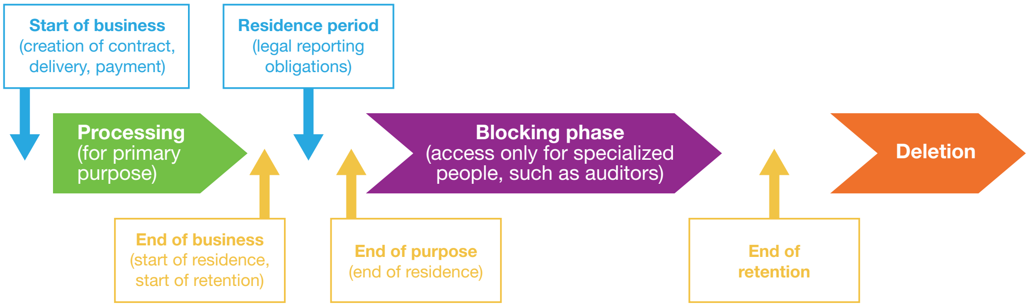
Start of business
(creation of contract, delivery, payment)
Residence period
(legal reporting obligations)
Processing
(for primary purpose)
Blocking phase
(access only for specialized people, such as auditors)
Deletion
End of business
(start of residence, start of retention)
End of purpose
(end of residence)
End of retention

Figure 2 The life cycle of personal data in business systems

These identity and access management features help support CCPA and GDPR compliance by minimizing access to personal information. In addition, by combining these features with SAP Access Control and SAP Process Control, you can ensure segregation of duties and organization policy management, which prevents users from having too many authorizations and enables further control over access to sensitive data.[6]

Erasing Data Once Its Purpose Is Complete

SAP Information Lifecycle Management (SAP ILM) features, which are embedded within SAP S/4HANA Cloud, help ensure that personal data has a life cycle from its beginning until the time it needs to be deleted, once its business purpose and all related legal obligations are complete (see **Figure 2**).

For the purposes of CCPA and GDPR, the retention time for data depends on its purpose. For example, let's say that you sell books and medicine online and a customer decides to purchase them, pays you for them, and has them shipped. For this purpose, a sales order will exist, then an invoice and payment, followed by a delivery arrangement. Once the delivery is complete, the transaction is complete. How long do you store the business partner's details (master data) and transactional data in this case?

The business rules that apply for selling books would be different from those for selling medicine — for example, selling medicine would require you to keep certain data for perhaps 10 years, while data from selling books would need to be retained for maybe two years. These rules can be made aware to SAP ILM, which can then use these rules to handle the retention and deletion of the data in an automated way to help you maintain compliance with CCPA and GDPR requirements.[7]

Providing Information to Subjects About Their Data

Under GDPR and CCPA, an individual has the right to know what data about them is collected and for what purpose it is being used. SAP S/4HANA Cloud includes an information retrieval framework that supports this requirement by enabling you to provide information to data subjects or consumers.

This information retrieval framework can be used to look for data about a business partner according to the purpose for which it was collected. The identified information can then be downloaded in an easy-to-read format and handed over to the data subject.[8]

[6] More details on the identity and access management functionality within SAP S/4HANA Cloud are available at http://bit.ly/S4HANACloudIAM.

[7] Find more information about the SAP ILM features embedded within SAP S/4HANA Cloud at http://bit.ly/S4HANACloudILM.

[8] Learn more about the information retrieval framework within SAP S/4HANA Cloud at http://bit.ly/S4HANACloudInfoRetrieval.

Proving Accountability via Technical and Organizational Measures

Features such as change logs, user or identity and access management logs, and application logs, which are included with SAP S/4HANA Cloud, can help you prove the integrity of your system and data as well as your accountability for that integrity. Read Access Logging (RAL), for example, helps you monitor access to sensitive data — you might want to know who accessed the social security number or bank account information of a certain individual, for instance, and there could be cases where you need to report this information to authorities.

These logging features support CCPA and GDPR compliance by helping to ensure the integrity of data and systems — for instance, the logs can be checked on a regular basis to detect malicious intent, such as too many unsuccessful login attempts by an employee on vacation. Under CCPA and GDPR, just like all processing, logging read access to data must have a purpose and must be done only when there is an absolute need to do so — for example, during year-end closing, an organization might need to track access to financial records. The RAL feature can be configured according to your business needs, and the logs then can be reviewed and managed using SAP ILM.[9]

SAP S/4HANA Cloud also includes features for building organizational models, which is another way to prove your accountability. Organizational models allow you to organize entities such as business units, people, products, sales organizations, purchasing organizations, and plants according to business needs by using line organizational attributes (such as company code, sales organization, and purchasing organization) and process organizational attributes (such as sales order types and delivery types) to classify people and processes. The better organized these entities are, the better grasp you will have on other aspects, such as authorizations and SAP ILM.

Summary

With GDPR in effect since May 2018 and CCPA due to roll out in January 2020, data protection continues to be a pressing issue. Regulatory requirements will also continue to evolve — in addition to new regulations likely to come, existing ones will change. For example, some aspects of CCPA are under discussion and could be amended in the near future.

Complying with data protection regulations such as GDPR and CCPA requires comprehensive and involved discussions across the organization and has a considerable impact on a company's business and technical landscape. While in this article we have only scratched the surface in terms of the SAP S/4HANA Cloud features that can help you toward your compliance goals, with the foundational information provided here, you will be well prepared to begin these discussions and further explorations within your own organization. ■

Learn More

- SAP S/4HANA Cloud Features for Minimizing Data Access: Identity and Access Management
  http://bit.ly/S4HANACloudIAM
- SAP S/4HANA Cloud Features for Erasing Data: SAP Information Lifecycle Management
  http://bit.ly/S4HANACloudILM
- SAP S/4HANA Cloud Features for Providing Information: Information Retrieval Framework
  http://bit.ly/S4HANACloudInfoRetrieval
- SAP S/4HANA Cloud Features for Proving Accountability: Read Access Logging
  http://bit.ly/S4HANACloudRAL
- SAP Best Practices for ILM
  http://bit.ly/BestPracticesILM
- SAP Best Practices for Data Protection and Privacy
  http://bit.ly/BestPracticesDataProtection

[9] More information about the RAL functionality embedded within SAP S/4HANA Cloud is available at http://bit.ly/S4HANACloudRAL.