AICPA CITP Credential Examination Series

Topic: SOC 2 Privacy Principle

Presenter: Jeff Cook

Jeff Cook: On behalf of the AICPA Information Management & Technology Assurance Division, this is Jeff Cook, and I'm here to talk about the SOC 2 Privacy Principle. I work for a cyber-security focused CPA firm called Veris Group, and in particular our expertise is around SOC reporting, and that's what I'm going to talk to you about today. In particular, we're going to talk about SOC 2 and the new privacy principle, which was revised recently with the issuance of TSP 100 from the AICPA, Trust Service Principles and Criteria, number 100.

This revision not only was for privacy but also it had some changes in the common controls, availability, confidentiality and processing integrity.

There was a lot of wording changes to this revision of TSP 100, and we're not going to get into a lot of those and the other principles, but the biggest changes came in privacy because previously privacy was considered almost a herculean type effort to go through in a SOC 2 audit. The AICPA guide from 2015, it was still a 64-page document in there for privacy controls, and a lot of it repeated itself, it was confusing, it was based on generally accepted privacy principles and it just didn't go over very well. So, the AICPA definitely made some clarifications to this because now, if you look at it, the TSP 100 has simplified privacy to eight criteria with a total of about 20 control objectives, and that's what I'm going to start with. We're going to take a closer look at where those privacy objectives are now for SOC 2.

The eight criteria now for privacy in the TSP 100 are as follows. Number one, notice of communications and commitments and system requirements; two, choice and consent; three, collection; four, use, retention and disposal; five, access; six, disclosure and notification; seven, quality; and eight, monitoring and environment. So, let's go into each one of those just briefly to talk about them in a little more detail for those objectives that the AICPA is looking for that are associated with those criteria. Under notice and communications of commitments and system requirements. Really, that focuses on notice about, and any changes to, your company's privacy practices and commitments as well as the system requirements that you have for internal users, to your company's employees, to carry out their responsibilities. It's really focusing on that internal aspect to make sure that everybody's aware of what your privacy commitments are to your customers.

Number two was notice and consent. That's going to really focus on the choices that are related to collection, use, retention, disclosure and disposal of personal information to data subjects, and any of the related consequences for that. Consent has to be obtained from the data subjects themselves or an authorized person, if that's required, and is only obtained for the stated purpose that you have. The basis for the determination of any implicit consent has to be documented. Number three, collection. Personal information must be collected in accordance with privacy commitments and system requirements. If explicit consent is required, that consent must be communicated as well as the consequences of failure to provide consent for the requested personal information.

Number four, use, retention and disposal. The use and retention of the personal information that you have has to be limited to the purposes that are identified for your privacy commitments and your system requirements so you can't use their PII for things other than what you're stating you're going to use it for. And the disposal of that information needs to be secure and consistent with your commitments and system requirements. Number five, access. Data subjects, once they are identified and authenticated, are given the ability to review and access their stored personal information and, if requested, have to be provided with physical or electronic copies of that information.

If access is denied to a data subject, notice as well as the reason for denial has to be provided by you to the data subject. Data subjects are also allowed to provide corrected, updated or appended information and that information is to be communicated to appropriate parties. If such corrections are denied for any reason you also, there, would have to provide notice as well as the reason for denial to the data subject. In number six with disclosure and notification, the personal information of data subjects must have the consent of the data subject prior to disclosure of the information to any third party.

Your company creates and retains authorized disclosure records that are complete, accurate and timely. Your company has to create and retain unauthorized personal information disclosure records that are complete, accurate and timely. This includes any breaches. Vendors or third parties that you're using whose products or services are part of your system and have access to personal information must comply with company privacy, commitments and systems requirements. If those vendors or third parties have an actual or suspected unauthorized disclosure of personal information, they must notify appropriate personnel at your company and act on that event to meet any established incident response procedures, privacy commitments or system requirements.

The notification of breaches and incidents must be reported to the affected data subjects, regulators and others as deemed necessary to know. A data subject can request and you must keep an accounting record of any personal information held and disclosure of that information. Number seven, quality. Personal information should be kept accurate, up-to-date, complete and relevant. Number eight, monitoring and environment. There must be a process for receiving, addressing, resolving and communicating the resolution of inquiries, complaints and disputes from data subjects and others.

Compliance with privacy commitments and system requirements should be periodically monitored and corrections and other necessary actions related to identifying deficiencies are taken in a timely manner. A lot of what happens with these new criteria and the related objectives are revolved a lot around policies. I can't stress enough the importance of having strong policies in your company, not only related to the system itself, which you're going to be used to under the other criteria for a SOC 2, but as well as these privacy commitments that you have. These notice choice and consent policies, disclosure of information, disposal of that information, how is it being used, what's the purpose, that all needs to be very clear when you are doing these privacy commitments and if you're going to go down the privacy road for SOC 2.

Another thing that the AICPA provided in TSP 100 is a mapping from the old GAPP methods and in this case GAPP meaning General Accepted Privacy Principles, to their new TSP 100 criteria. Let's talk about an example here, under the old GAPP 1.2.10, it talked about privacy awareness and training. That is now considered to be included in common criteria CC 2.3, which is the responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties. What is that telling us, that's telling us that not only did the AICPA map the old GAPP to these new criteria that I just talked about, but also that they mapped some of the old GAPP to the existing criteria such as this common criteria here.

Some other considerations that you would have for adding the privacy principles I think would be in your section three, which is your system description. That's going to be very important for you to talk about some of the policies I mentioned before that you're going to have to put in place to meet those control objectives, but also some of the other areas of section three. Let's talk about that in more detail. For example, when section three talks about the types of services provided, you're going to want to talk potentially about services that deal with personal information. Under section three procedures, this one is critical because you're going to have to talk about procedures that are related to those control objectives that I discussed earlier and how the company is dealing with that.

For example, when you have the notice choice and consent, what are the procedures for providing that notice? For giving the choices? For getting the consent from the end user? For data? You're going to want to expand on that in your section three, you're going to want to talk about what's considered personal information or PII at this point, how you capture significant events and conditions. Similar to procedures, it's going to be how you're capturing events and conditions related to certain privacy controls that we talked about earlier. In a minute I'm going to talk about some service organizations and user entity controls. That's going to be any discussion of the privacy controls that we haven't discussed as well as risk assessment process including privacy considerations, how did your risk assessment get affected by these privacy considerations that you now have.

For sub service organizations, it's going to be similar to what you have to do already, but you have to give consideration to how your sub service organizations are helping you meet the privacy principle objectives. If the sub service organization, or a third party, has access to or is permitted to view the PII, compliance with your own privacy policies and commitments and system requirements has to be considered, but also you need to consider the privacy practices of the sub service organization. How are they handling that PII? When the PII is no longer needed, how do they dispose of it? How are they retaining it? How are they making sure it's secure? Those are the things you're going to have to consider.

With complementary user entity controls, service organizations are going to have to consider if a more complementary user entity controls are going to be needed for section three of the SOC 2 report. For example, if you're providing information to a hospital, perhaps there's some complementary user entity controls that the hospital has privacy policies themselves for notice, choice and consent. Another could be proper disposal of personal information after the information has been used. While

this is still a large effort for SOC 2, the new TSP 100 definitely has made the process simpler and more streamlined.

Companies that are subject to other frameworks like let's say HIPAA or HITRUST, will now find SOC 2 privacy principle allows for more of those single compliance audit efforts with multiple reuse results to be more possible because it's more simplified. To summarize, we talked about the new criteria that are required for privacy, those control objectives that are related to those criteria and how it's going to be a little bit easier for you to get that in your SOC 2 now. I wouldn't say it's going to be an easy effort overall, but definitely the AICPA has made some improvements here on how to get that privacy principle working for you.

On behalf of the AICPA Information Management & Technology Assurance Division, this has been Jeff Cook and I just presented on the SOC 2 privacy principle. To access more information and resources on SOC reporting and related information technology and technology assurance, visit aicpa.org/imta/resources. I also highly encourage IMTA section members and CITP credential holders to review your bi-weekly electronic IMTA news, to keep up with the latest news, resources, advocacy and events. Visit aicpa.org/imta/news for the latest edition.

Disclaimer

This podcast is designed to provide illustrative information with respect to the subject matter covered, and does not represent an official opinion or position of the AICPA or AICPA.Org. It is provided with the understanding that the AICPA and AICPA.Org are not engaged in offering legal, accounting or other professional service. If such advice or expert assistance is required, the services of a competent, professional person should be sought. The AICPA and AICPA.Org make no representations, warranties or guarantees as to, and assume no responsibility for, the content or application of the material contained herein, and especially disclaim all liability for any damages arising out of the use of, reference to, or reliance on such material.