2021-04-13 Security, Privacy and Data Protection Drafting Group Meeting Notes

Attendees

- Chuck Curran
- Drummond Reed
- Jan Lindquist
- Kaliya Young, WG co-chair
- Pagona Tzormpatzidou, chair
- Peter Davis
- Scott Perry
- Trev Harmon, PM
- Xavier Vila
- Zsombor Szabo

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Trev
5 min	Review of the template	Pagona
	Topic discussions	Everyone
3 min	Wrap up	Pagona

Recording - *Link*

Notes

- DId the IP / antitrust announcement
- We are going to start with a review of the template.
- Drummond mentioned different groups are using the template in different ways.
- How do we want to handle the phasing approach outlined in the template, especially as our group is going to be dealing primarily with principles.
- We may be able to pull over content from our current KIQ document.
- Drummond, wearing his governance framework hat, would like recommendations that will end up in the governance framework. These would include MUST, SHOULD, and MAY statements.
- Jan had a call with Scott to get a consensus about how we bring in the governance work. Jan is working on privacy, and Scott is working on a higher level.
- Scott said that one of the things that needs to be asked regarding the governance framework is does it require a risk assessment, and does it require that sub-governance frameworks also have a risk assessment.
- The decision that they made was that we did need to have a risk assessment based on ISO 27005 requirements. That proposal has been posted by Scott to the other groups for feedback. There is a hope that this will be a discussion point in tomorrow's Leads meeting.
- There was a discussion regarding where the work of the risk assessment would live in the current drafting groups. Our group will certainly need to provide input on this.
- Scott mentioned that we are trying to limit / mitigate the risks associated with these transactions. We need to be identifying the risks.
- Pagona noted that if we want policy makers and regulators to look at our work, there needs to be a recognition of how that currently works in privacy regulation.
- Jan has interest in us looking at the notice receipt work that has been done at Kantara. This would be relevant for all three zones.
- Our document does need a table of contents to provide an overview.
- Had a short discussion regarding levels of assurance.
- Drummond asked about integrating in privacy by design principles. Peter asked about the IP rights regarding the proposed content. He is going to put it in the Google Drive as a submission.
- There was a question regarding who the audience is for the deliverables. https://docs.google.com/document/d/1uml0h7ImzHaZnQPiauhICr_3aztloWVcNRe0K67xKAo/edit?usp=sharing
- Drummond provided an overview of the differentiation between a "credential" and a "pass" in the way we are using it. A pass is meant to be the minimal information needed to do a particular action.
- Chuck brought up the article last week's Washington Post.
- Pagona brought up that in our data minimization section we need to consider levels of assurance and context to determine what requirements we put forward.
- Jan asked if Drummond was looking for machine-readable or human-readable policy statements. Drummond is primarily looking for the human-readable form of governance policies, but we could provide additional example privacy policies.
- Chuck noted that there is a high degree of variance with model privacy policies across jurisdictions. It may be difficult to do more than statements of "my adhere to applicable laws". Pagona seconded that.
- Chuck brought up the data sunsetting / discarding of data. This has not only been brought up in the EU, but also now in the US government. Our document needs to address this. It's not the technology that gets sunsetted, but the data. Policy makers are going to be looking for this.
- This conversation is also related to data retention, as well.
- We'll pick up the conversation on Thursday regarding what our position is going to be on the proposals and approaches to sunset data.

Chat Log

00:10:21 Trev Harmon: The template: https://docs.google.com/document/d/15GZHet3CZF2-gBuyH7JOSLviVc4fubmvQ9uK1tLOBI8/edit
00:12:01 Drummond Reed: I agree that the phasing approach may not be relevant to this group. It may be only the expectations on conformance.
00:17:18 Scott Perry: At least it will map to Information Trust Rules
00:18:47 Drummond Reed: Yes, I expect most of the policies from this DG will map into the Information Trust Rules section.
00:43:05 Drummond Reed: Audience description: https://docs.google.com/document/d/1uml0h7ImzHaZnQPiauhICr_3aztloWVcNRe0K67xKAo/edit?usp=sharing
00:47:16 Drummond Reed: that’s a model policy right there: “Any verifier that does not need personal data to make a trust decision MUST NOT request or retain any personal data beyond what is necessary to authenticate the credential or pass holder.”
00:58:17 Drummond Reed: There is a flip side to the coin—these credentials are personal health records which in principle belong to the individual.

Action Items