2021-04-08 Security, Privacy and Data Protection Drafting Group Meeting Notes

Attendees

- Abdul Sattar
- Drummond Reed
- Jan Lindquist
- Kaliya Young, WG Co-chair
- Lisa Rabenau
- Michael Becker
- Pagona Tsormpatzoudi
- Peter Davis
- Robin Renwick
- Trev Harmon
- Zsombor Szabo

Agenda Items

Time	Item	Who
2 min	Welcome & Antitrust Policy Notice	Trev
10 min	Review of Work to Be Completed	Pagona
	Discussion on Principles	Everyone
3 min	Wrap up	Pagona

Recording - *Link*

Notes

- Did the IP / antitrust announcement.
- The Google document is the place where everyone can put their ideas, regardless of structure. We'll be editing the input, so don't worry about format right now.
- We are meeting on Tuesdays and Thursdays at the same time
- We need to have all of the main ideas into the document; otherwise we won't have enough time to edit.
- Reviewed the timeline for the next couple of months.
- Reviewed the three different zones.
- Reviewed the set of principles listed in the Google document.
- Had a discussion regarding data minimization.
- Discussing data binding, Drummond noted:
    - Zone 1 is all about gathering the data regarding the event.
    - Zone 2 deals with identity binding as part of the credential issuance, as Zone 3 needs to be able to know that the credential belongs to the specific person.
- The level of assurance in Zone 3 cannot be any higher than the level of assurance done in Zone1 and Zone 2. Zone 2 can add additional binding information, which may raise the level of assurance.
- Peter asked why we would want to entangle data minimization requirements with levels of assurance.
- We talked through how the principles apply across the zones:
    - Zone 1: Don't collect more information than you need.
    - Zone 2: Don't collect more information than you need to do binding.
    - Zone 3: Don't ask for more information than you need.
- Had a discussion regarding data quality.
- Peter pointed out that regulation tends to require this (e.g., GDPR requires that data be accurate, and that there is a method by which to correct incorrect data).
- Had a discussion regarding consent and the related data. It was proposed that we document requirements for the recording of notice and consent.
- The risk assessment needs to be part of the governance framework.
- Had a discussion regarding how one proves that a specific solution meets security and privacy requirements.
- The individual needs to be at the center of all of this.
- The GHPC Steering Committee has recently had conversations regarding both a certification program and a test suite.
- The Governance Framework group is also looking at a method for certifying other frameworks.
- Discussed how certification would work may apply.

Chat Log

```
00:04:14        Michael Becker:        Sorry!!!!
00:06:32        abdul sattar:        can you please share google drive.  apologies, I might have missed the link
00:06:40        Drummond Reed:        Great point. Which document should we be contributing to?
00:06:50        Trev Harmon:        https://docs.google.com/document/d
/1_gnVGOrlT59cNwiZlZJb3RTO90GrRIbS7bd39b3DJiE/
00:24:35        Drummond Reed:        In Zone 1 and Zone 2, data must be collected in order to administer the
health event and to issue the credential or pass. In those zones, data minimization applies to data collection.
00:26:15        Jan Lindquist:        would like to double check the agenda. had a couple of suggestions for
work in the group which is at the bottom of the google doc. It might be touching on some of the questions in a
structured approach.
00:32:00        Robin Renwick (IE):        False positives/false negatives that automatically issue a cert
/record in Zone 1/2 would be a concern.
00:48:54        Drummond Reed:        +1 to "individual at the center"
```

Action Items

1. All main ideas need to be in the document by Friday, April 16th.
2. Jan to bring information next time regarding defining code of conduct.