Privacy Connect Project

Introducing GEPS!

Fall 2018
• Project 3: Global Education Privacy Standard (GEPS)
  - Establishing contractual agreements over the protection of student data is only the first step. Districts want to know if/how providers are meeting the requirements and solution providers are asking “How should we meet these contractual requirements”?
  - In order to create a secure K-12 environment we need to connect the contractual obligations to real world technology solutions – not “industry best standards” as currently stated in many data privacy agreements (DPA).
  - Privacy Connect will connect contract clauses to privacy obligations to technical benchmarks so all stakeholders have common understanding and expectations around how privacy obligations are being met.
Project 3: SDPC Tactical Privacy “Connect”

**Goal:** Support data stewards and their institutions to address student data privacy from application identification to application utilization.

- **Application Vetting** (Digital Tools Governance/SDPC App)
- **Privacy Contract Wording** (Contract Builder)
- **Technical Requirements** (Technical Standards)
- **Workflow Automation** (SDPC Application)
  - Automate Data Exchanges via Privacy Requirements (TBD)
- **Stakeholder Communications at Each Step**
SDPC Project 1 – “Baby Steps”
SDPC Value Add: “Privacy Connect”

- “Secure/Quick Connections”
- Privacy Standards
- Certification

Distances

Vetting & Contracting Framework

Integrators

Integrators

Marketplace Products
Global Education Privacy Standard (GEPS)

School / Department of Education
(Data Controller)

Written Contract
Clause 1
Clause 2

Contract Obligations Pool
Contract Obligations
Obligation 1
Obligation 2

Legal / Policy
Control Benchmark Sets
SDPC Set
Other Sets

Technical
Privacy Obligation Document (POD)
Obligation 1 XML
Obligation 2 XML

Vendor
(Data Processor)

NIST/ISO/IEEE
“Other” standards

Global Education Privacy Standard (GEPS)
**Clause**: Provision included in a written agreement or contract. A contract clause will address an aspect of the contract between parties, detailing the agreement to ensure all parties understand what is expected of the other.

**Contract Obligation Pool**: The comprehensive set of Obligations to choose from to align to any and all of the Contract Clause requirements and the responsibilities a Data Controller (Educational Organization) and Processor (Vendor/Supplier)

**Contract Obligations**: A term that encapsulates all of the responsibilities a Data Controller (Educational Organization) and Processor (Vendor/Supplier) must meet in order to protect the interests of the Data Subject (Learner) and can include reference to an underlying contract which covers the data transaction and handling of the data by the recipient. (A4L Community 2018)
**Control Benchmark**: A set of technical effective practices for controlling the access and usage of sensitive data. Control Benchmarks encompass such technologies as encryption, network authentication, access control lists (ACLs), file integrity auditing software, etc. and ideally are developed through a set of Community-driven processes comprised of end users, marketplace providers, and privacy/security professionals (CIS).

**Privacy Object Document (POD)**: A group of Obligations codified for machine readability.

**Privacy Object**: Object is a technical representation of an Obligation (referring to data terms such as object, attribute, element).

**Global Education Privacy Standard (GEPS)**: A PK-20 global set of data privacy obligations (obligations) that can be aligned to contractual clauses as well as technical control benchmarks. GEPS includes open XML code (PODS) to transfer privacy obligations between controllers and processors to bridge the gap in understand of education data protection expectations.
<table>
<thead>
<tr>
<th>Obligation</th>
<th>US Privacy</th>
<th>AU Privacy</th>
<th>EU GDPR</th>
<th>Discussion</th>
<th>DPO Terms &amp; Application</th>
</tr>
</thead>
</table>
| **Data cannot be used for advertising or marketing purposes** | Article IV, Section 6. Advertising Prohibition. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose | APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing. | Rec.70; Art.21(2)-(3) Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling | The limitation on the use of data by Data Processors for marketing or advertising purposes in consistent in all locales.  
In the U.S. agreement it is prevented outright, in the AU whilst limited, exceptions do apply. The GDPR provides individuals with the right to opt out. | “Data able to be used for marketing purposes: “Yes/No”, Data Processor Marketing contact name, Marketing contact email, Marketing contact phone number”  
The “Data able to be used for marketing purposes: Yes/No” and Data Processor marketing contact details would be a series of elements in the DPO object.  
Technically Data Processors would do nothing however the contents of this entry (as part of the DPO) could be made available to the Data Subjects (eg via the SDPC website) and allow them to contact the Data Processor and opt out from marketing/advertising processes. |
How Are We Communicating the “What”

There are many if not an infinite number of potential use cases. We want to ensure that WE:

1) Build directly upon the success of the SDPC.
2) Answer vendors' most common and immediate question - "How do you expect us (the vendor) to meet these privacy obligations?"
3) Answer the districts' most common and immediate question - "How do we know vendors are meeting these contractual obligations?"
4) Provide a tool that is flexible for future growth of functionality to potentially address use case nuances and a variety of views on "Control Benchmark Sets"
5) Develop an OPEN tech standard to convey privacy obligations and control benchmark expectations across the wire (PODS)
The current goal is to keep the first deliverable actually achievable with a few simple scoping decisions for phase 1. **WE WILL;**

1) Focus on the SDPC Alliance contracts aligned to the National Model (CA, WA, OR, TX, MA, ME, VT)

2) Assume (and this is a big one) that for the purpose of establishing obligations, the use case is the same for these standard contracts with no edits, across all districts. The use case is defined by the contract.

3) Create a recommended set of control benchmarks but allow other organizations to define their own (such as the state of NY adopting NIST 800 171 r1).