Technical Privacy

Workshop: Thursday, March 15, 2018
1:45-2:45

Presenters: Anthony Yaremenko, NSIP and Mike Reynolds, CedarLabs
We take privacy very seriously here.
Technical privacy controls

- Scope of work
- Who’s involved
- Approach
- GDPR, Privacy by Design
- What’s agreed currently
- What we’re debating
- Your thoughts
- Next steps
Scope of work
Who’s involved?

- US
- UK
- AU – All States/Territories (inc NZ), Non-Gov sector
- Functional group: Data Privacy
- Functional group: Infrastructure
Approach

- Focus on the most current global work in this space
- General Data Protection Regulation (GDPR)
- Why GDPR?
  - Current/recent approach (May 2018)
  - Scope of individuals
    - Protect rights of Europeans
    - Applies regardless of where data is collected
  - Impacts for many US, AU, NZ organisations
GDPR

- Applies to all businesses, organizations, sectors, situations, and scenarios, regardless of a business’s size, head count, or financial turnover.
- Requires ‘Privacy by design’ focus
Privacy by Design

1. Proactive, not reactive
2. Privacy must be default setting
3. Embedded into design
4. Positive sum, balance between privacy & security
5. End-to-end lifecycle protection (minimize, retention, deletion)
6. Standards visible, transparent, open, independently verifiable
7. User-centric: granular options, maximise safe defaults, detailed notices, user-friendly, clear
Data Subject
- A natural person whose personal data is processed by a controller or processor
Privacy concepts

Data Controller
- A person or an entity, such as you or your organization, which decides what data is collected, how it is used, and whom it is shared with.
Privacy concepts

**Data Processor**
- Any entity other than the data controller who processes the data
Data Protection Obligation
- Defines what data, what can be done with the data, how is it to be respected
Privacy concepts

- Subject
- Data shared by data subject
- Controller
  - Can only collect data for a specified, explicit, legitimate purpose
- Data shared by data controller
- Processor

***Credit to Jon Nicholson for diagrams and documentation on GDPR and DPO***
GDPR Requirements

1. Whenever a controller uses a processor it needs to have a contract in place.
2. The GDPR sets out what needs to be included in the contract.
3. Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide ‘sufficient guarantees’ that the requirements of the GDPR will be met and the rights of data subjects protected.
4. Processors must only act on the documented instructions of a controller.
Approaches to address privacy

- Encrypt data in transit
  - Can encrypt data prior to transmission
  - Can use encrypted connection
    - HTTPS
    - SSL/TLS
    - FTPS, SFTP
- Encrypt data at rest
  - Encryption of key fields (usernames, passwords, contact details)
  - Encrypt storage drive
What’s agreed that SIF offers so far

- SIF supports encryption of data in transit (TLS)

- Proactively identify at-risk data and priorities for protection in transit and at rest
  - SIF Data model enables this conversation

- Step further, AU have classified all SIF data objects and elements see:
  http://specification.sifassociation.org/Implementation/AU/3.4.3/1/
Thinning out the wildebeest herd...
Proposed data protection in SIF

• DPO defined via infrastructure object, locale agnostic
• Setup via utility service
• Implemented in agent (eg redaction) or 3rd party library
• Agent’s responsibility to first obtain DPO obligations prior to other, line-of-business data requests
• Agent’s responsibility to monitor for DPO events
**DPO – How it would work**

1. I’d like data please

2. Agent checks for DPO and ‘open’ or ‘closed’ setting

3. We have a DPO in place, please obtain to get the ‘rules of the game’

*Default is always ‘closed’*
DPO – How it would work

4. What’s the DPO please?

5. DPO consumed by processor

6. DPO evaluated by processor
DPO – How it would work

1. Request current students

2. Agent checks DPO, only student preferred name initial and surname initial allowed

3. Filtered and transformed student data consumed by processor

4. Student data treated in accordance with DPO

5. Eg delete after 30 days, don’t forward etc
Data Protection Obligation

<dataProtectionObligation id="" status="APPROVED" approvalDate="" effectiveDate="" expiry="P30D">
  <name>StrawMan</name>
  <description>Second straw man for data privacy obligations/advice/terms</description>
  <zone></zone>
  <objectName></objectName>
  <fingerprints>
    <fingerprint></fingerprint>
  </fingerprints>
  <contexts>
    <context>default</context>
    <context>pre-enrol</context>
  </contexts>
</dataProtectionObligation>
<identifiers>
  <!-- This needs to have the case of refIds referencing different types of object, e.g. PersonPicture in SIF UK 2.0 -->
  <identifier name="@refId"></identifier>
  <identifier name="@workforcePersonalRefId"></identifier>
</identifiers>

<servicePaths>
  <servicePath>/persons</condition>
  <servicePath>/schoolGroup/class2/persons</condition>
</servicePaths>

<policy>
  <namespaces>
    <namespace>
      <prefix>sifus</prefix>
      <pattern>http://sifassociation.org/datamodel/US/3.*</pattern>
    </namespace>
  </namespaces>
  <defaultRights>
    <right type="QUERY">REJECTED</right>
  </defaultRights>
  <terms>
    <term ttl="how long I can keep the data once receiving it">
    
    <target>/sifus:person</target>
    <rights>
      <right type="QUERY">APPROVED</right>
    </rights>
  </term>
</terms>

</policy>
What we are now doing

• Work through high level **business concerns** regarding privacy & security

• Determine what is the appropriate response from A4L:
  • Something A4L cares about and can fix now
  • Something A4L cares about and will fix in (x) time period with the following approach (y)
  • A concern best handled via privacy contract (refer SDPC)
Related privacy work

• SDPC
  • Project 1: Privacy contract framework
  • Project 2: Digital governance tool
  • Project 3: Privacy connect
What we don’t want

Cruise the Net faster with 2 wheels

rolloine

COMPUTER ACCESSORIES

Ddpf faster than others

1 Wheel Scrolling Mouse

Scrollware Included

Windows®

® wheel functionality
## Data protection obligations - workshop

<table>
<thead>
<tr>
<th>#</th>
<th>Requirement</th>
<th>Obligation</th>
<th>US</th>
<th>UK</th>
<th>AU</th>
<th>NZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Delete data after a period of time</td>
<td>Add “Data expiry” rule, n days</td>
<td></td>
<td></td>
<td>No federal law, will check local</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Data processor obtains data they are not entitled to</td>
<td>Add “Data issues notification contact” email address. Notify if issue.</td>
<td></td>
<td></td>
<td>APP 4</td>
<td></td>
</tr>
</tbody>
</table>
How can you help?

- Grab a piece of paper
- Write down your country/region eg U.S., California
- List at least 3 privacy related concerns you have in the education domain
- Against each write down what you believe the solution should be from an A4L perspective
Next steps

- Based on workshop, expand scope of business concerns and proposed approach from A4L
- Workshop broadly with community
- Develop technical solutions via SIF framework
- Develop contractual / business solutions in consultation with SDPC
Thank-you!

Thanks for your contributions and support
Great links

- https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/