Privacy by design – privacy by default

Kevin Shaw, Head of Information Security

September 2017
INTRODUCTION

• Aims
  – Introduce the seven principles of Privacy by Design
  – Discuss what this could mean for the University
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

The seven principles

1. Proactive not reactive; Preventative not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality – positive sum, not zero sum
5. End to end security – lifecycle protection
6. Visibility and transparency
7. Respect for user privacy
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle one: Proactive not reactive

1. Proactive not reactive; preventative not remedial
   – Aims to avoid events before occurring
2. Privacy as the default
   – Purpose specification
   – Collection limitation
   – Data minimisation
   – Use, retention, and disclosure limitation

All privacy matters are built in to the system or are process driven
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle three: Privacy embedded into design

3. Privacy embedded into the design

– Privacy by Design is embedded into the design and architecture of IT systems and business practices
– Not “bolted on” or after the fact
– Privacy becomes an essential component of the core functionality being delivered
– Privacy is integral to the system, without diminishing functionality
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

The information life cycle

Creation / development → Storage → Transmission / distribution → Archive → Destroy
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle four: Full functionality

4. Full functionality: positive sum, not zero sum
   - Privacy by Design seeks to accommodate all legitimate interests and objectives avoiding unnecessary trade-offs
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle five: End to end security

5. End to end security – lifecycle protection

– Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish

– Ensure that all data is securely retained, and then securely destroyed at the end of the process, in a timely fashion

– Privacy by Design ensures cradle to grave, secure lifecycle management of information, end to end
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle six: Visibility and transparency

6. Visibility and transparency
   - Accountability
   - Openness
   - Compliance

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is legally verifiable and subject to independent verification.

Its component parts and operations remain visible and transparent, to users and providers alike.

Principle of “trust and verify” applies.
PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Principle seven: Respect for user privacy

7. Respect for user privacy
   – Consent
   – Accuracy
   – Access
   – Compliance

Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Keep it user-centric.
### WHAT THIS MEANS FOR THE UNIVERSITY

<table>
<thead>
<tr>
<th>Principle</th>
<th>University action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Proactive not reactive; Preventative not remedial</td>
<td>Project / Programme Management Governance and initiation</td>
</tr>
<tr>
<td>2. Privacy as the default</td>
<td>Privacy as a standing item on business cases</td>
</tr>
<tr>
<td>3. Privacy embedded into design</td>
<td>Privacy by Design policy</td>
</tr>
<tr>
<td>4. Full functionality – positive-sum, not zero-sum</td>
<td>Data Protection Impact Assessment (DPIA)</td>
</tr>
<tr>
<td>5. End to end security – lifecycle protection</td>
<td>Encryption – end to end</td>
</tr>
<tr>
<td>6. Visibility and transparency</td>
<td>Process to make Information available – preference panels?</td>
</tr>
<tr>
<td>7. Respect for user privacy</td>
<td>Privacy notices and University culture</td>
</tr>
</tbody>
</table>
YOUR QUESTIONS