Privacy by Design and the GDPR

ISACA Geek Week – Atlanta
August 9, 2016

Phillip Mahan, CISA, CIPM, CISSP, CIPT, CIPP/US, CCSK
Director, Office of the CPO
Ionic Security
Standard Disclaimer

The presenter of this information may or may not be a Lawyer, and even if they are, they are not YOUR lawyer. Nothing that is said should be considered legal advice or opinion. The information presented herein represents the speaker’s personal opinion and current understanding of the issues involved. Neither the speaker nor their respective organizations assume any responsibility or liability for damages arising out of any reliance on or use of this information. The presenter is not speaking on behalf of any Company where they are currently, or have in the past been employed.

If you are viewing this presentation from a distribution rather than actually being there, some of the slides may not make sense out of context. If you have questions, please contact the presenter(s) at the address provided on the contact slide.

Thank you
Privacy is not dead. It’s not even mortally wounded. However, in a world with an Internet full of things, we need a guide. A way to view the design and creation of our systems that will allow for data to be collected and used in a manner that will keep us protected.

When the EU was formed, Privacy was added to its charter as “a fundamental Human right”.

The world has changed. Technology has changed. The desire for Privacy has not.
Privacy by Design
[Information and Privacy Commissioner of Ontario www.ipc.on.ca]

Created in the 1990’s to meet a need.

Developed by Dr. Ann Cavoukian.

Adopted into EU Regulations For Data Protection

Adopted into EU Regulations For Data Protection
General Data Protection Regulation
[Regulation (EU) 2016/679]

• Deals with “the protection of natural persons with regard to the processing of personal data and on the free movement of such data”
• Becomes Effective on May 25, 2018
• Has a reach that extends far beyond the borders of the EU
• Privacy by Design and by Default is a GDPR Requirement
• Contains 99 Articles within 11 Chapters
General Data Protection Regulations

- Chapter 1 – General Provisions
- Chapter 2 – Principles
- Chapter 3 – Rights of the Data Subject
- Chapter 4 – Controller and Processor
- Chapter 5 – Transfer of Personal Data to 3rd Countries or International Organizations
- Chapter 6 – Independent Supervisory Authorities
- Chapter 7 – Cooperation and Consistency
- Chapter 8 – Remedies, Liability and Penalties
- Chapter 9 – Provisions Relating to Specific Processing Situations
- Chapter 10 – Delegated Acts and Implementing Acts
- Chapter 11 – Final Provisions
## Privacy by Design Principles

<table>
<thead>
<tr>
<th>Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive not Reactive; Preventative not Remedial</td>
</tr>
<tr>
<td>Privacy as the DEFAULT</td>
</tr>
<tr>
<td>Privacy Embedded into the Design</td>
</tr>
<tr>
<td><strong>Full Functionality: Positive-Sum not Zero-Sum</strong></td>
</tr>
<tr>
<td>End-to-End Security: Lifecycle Protection</td>
</tr>
<tr>
<td>Visibility and Transparency</td>
</tr>
<tr>
<td>Respect for User Privacy</td>
</tr>
</tbody>
</table>
The GDPR has provisions which require controllers to assess risks presented by processing activities and to develop and implement adequate measures to address these risks.

(116) Relates to data crossing Union borders and data protection – [pg 22/88]

Specific Articles within the GDPR that address this principle:
- Article 5 – Principles relating to processing of personal data
- Article 24 – Responsibility of the controller
- Article 25 – Data Protection by Design and by Default
- Article 32 – Security of Processing
- Article 35 – Data protection impact assessment

“The time to learn to use a fire extinguisher is not when your kitchen is ablaze”
Privacy as the DEFAULT

In order to deliver the maximum degree of Privacy, personal data must be protected without action from the individual. GDPR has specific requirements to ensure the data subject does not have to take action in order for their data to be protected.

(78) Requires measures are taken by default to ensure that Regulation is followed. [pg 15/88]
(108) Compensating measures for safeguards in absence of an adequacy decision for third country should be taken by controller or processor. [pg 20/88]

Specific Articles within the GDPR that address this principle:
Article 25 – Data Protection by Design and by Default
Article 32 – Security of Processing
Article 39 – Tasks of the data protection officer (Ensures that rules are followed)
Privacy Embedded into the Design

Privacy Controls should be embedded in the architecture of IT systems, operations, and business processes without lessening functionality for the User.

(4) The processing of personal data should be designed to serve mankind. [pg 2/88]
(78) Producers of products processing personal data should take into account data protection with due regard to fulfil their data protection obligations. [pg 20/88]

Specific Articles within the GDPR that address this principle:
   Article 25 – Data Protection by Design and by Default
   Article 32 – Security of Processing
   Article 35 – Data Protection Impact Assessments
It is possible to have Privacy AND Security. This principle seeks to accommodate all legitimate interests and objectives in a ‘win-win’ manner, not in a way that encourages trade-offs.

Chapter 9 [Articles 85-91] Contain provisions for Specific Processing Situations
Embed Privacy and Data Protection into your systems throughout the data lifecycle Collection to Destruction.

Collection -> Use -> Disclosure -> Retention -> Destruction

This principle resonates throughout the GDPR in the following chapters:
Chapter 3 – Rights of the Data Subject [Articles 12 through 23]
Chapter 4 – Controller and Processor [Articles 24 – 43]
Chapter 5 – Transfer of Personal Data to Third countries or International Organisations
Visibility and Transparency

Assure all stakeholders that you are operating according to stated promises and objectives subject to independent verification.

The GDPR has gone to great lengths to ensure Visibility and Transparency, including:
Chapter 6 – Independent Supervisory Authorities [Articles 51 – 59]

Article 68 – European Data Protection Board
The Data Protection Board gives a voice to all Member States of the EU

Chapter 8 – Remedies, Liability, and Penalties [Articles 77-84]

Article 37 – Designation of the data protection officer
The DPO will give a place for your Data Subjects to have more Visibility into what Data is collected and how it can be corrected
The purpose for the GDPR is the protection of personal data for the citizens of the European Union. The EU Charter states that Privacy is a fundamental Human right.

Technology permeates all aspects of life, throughout the world, and we need to keep in mind the needs of the Data Subject, because after all, we are all the Data Subject at one point or another.

**Data Subjects need:**
- Strong Privacy DEFAULTS.
- Appropriate Notice as to what is being collected and why.
- User-friendly options to control their options.
- Choice and Consent for data collection, use, and disclosure.
- Consistency of adherence to the rules.
May 25, 2018 is Coming: Be Ready

- By embracing Privacy by Design, you will be better positioned to comply with the GDPR Regulations
- GDPR is the law of the land for the European Union, if you are a multi-national, learn to love it.
- Data Protection and Privacy are here to stay.
Questions?

Email: Phillip@ionic.com
Twitter: @Mahan_Presents

Thank you for your time today.

About Ionic Security
Ionic Security accelerates Internet trust by protecting and controlling data everywhere it travels and anywhere it resides, whether on the corporate network, in the cloud or on mobile devices. The industry's first high-assurance data protection and control platform, Ionic Security takes a comprehensive approach to protecting distributed data in today's borderless enterprise without proxies or gateways or changes in user behavior.

The platform has been licensed to millions of users worldwide in a wide range of industries including Financial Services, Public Sector, Retail, Healthcare, Enterprise Software and Manufacturing.

The company is headquartered in Atlanta, Georgia, and is backed by leading firms including Amazon.com, Inc., Goldman Sachs, GV (Formerly Google Ventures), Icon Ventures, Kleiner Perkins Caufield & Byers, Meritech Capital Partners, and TechOperators.