GDPR Changes

IEEE Region 8 Meeting

Sydney, Australia

12 August 2017

Agenda

- What is the GDPR?
- What is IEEE doing to comply with the GDPR?
- How will this impact Region 8?

Background

- General Data Protection Regulation (GDPR)
- EU regulation with respect to protection of personal data related to an individual
  - Replaces EU Data Protection Directive
- Effective as of May 25, 2018
- GDPR applies to all organizations worldwide when processing data related to EU citizens

Personal Data

- Any information that can either directly or indirectly identify a natural person/data subject
- Much broader than previous definitions
- Examples
  - Name
  - Photo
  - Email address
  - Posts on social networks
  - IP address

User Rights

- Right of Correction
- Right to Access
- Right to Withdraw Consent
- Data Portability
  - If asked, Data Controller must provide a copy of personal data in a commonly used and machine readable electronic format
- Right to Object
  - If Data Controller is processing data for direct marketing or profiling, the user may need to be informed and can object

User Rights (continued)

- Right to be Forgotten/Data Erasure
  - If asked, Data Controller must erase data and stop further distribution
  - Data Controller may be required to inform third parties to stop using previously provided personal data
  - Right is balanced against freedom of expression, public interest in health/scientific/historical research, and exercise/defense of legal claims

Consent

- Must be “freely given, specific, informed, and unambiguous”
- In cases of sensitive data, must be explicit
- Implied consent, opt-out, conditional/required consent, and cumbersome terms and conditions are no longer permissible
- Existing consent will only work if it meets the new requirements

Consent (continued)

- Consent can only follow disclosure to data subject of:
  - Nature of data being collected
  - Purpose of processing
  - Identity of data controller
  - Recipients of personal data
  - Duration of retention

Data Controller Obligations

- Under Article 32 Data Controllers must:
  - "Implement appropriate technical and organizational measures"
  - Take into account "the state of the art and the costs of implementation"
  - Must also consider "the nature, scope, context, and purpose of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."

Security Action Mitigation

- The pseudonymisation and/or encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Challenges

- Organizations must be able to demonstrate compliance
- Data breach notifications
  - Must happen without "undue delay" within 72 hours of becoming aware of issue
  - Required, with some exceptions, for accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access
  - Notice process is currently a bit unclear

Consequences

- Regulators can impose temporary processing bans, require breach notification, or order erasure of personal data
- Fines
  - Up to 4% of global turnover or EUR20 million; whichever is higher

What IEEE is Doing

- Formed a cross OU taskforce
- Catalogued and characterized data collected and consent used to obtain it
- Developing strategy to improve consent obtained
- Privacy Impact Assessments
- Develop implementation strategy and associated budget
- Review policies and notices
- Institutionalize privacy by design in development
- Appointment of DPO
- Understand how to respond to users enforcing rights
- Prepare for data breaches

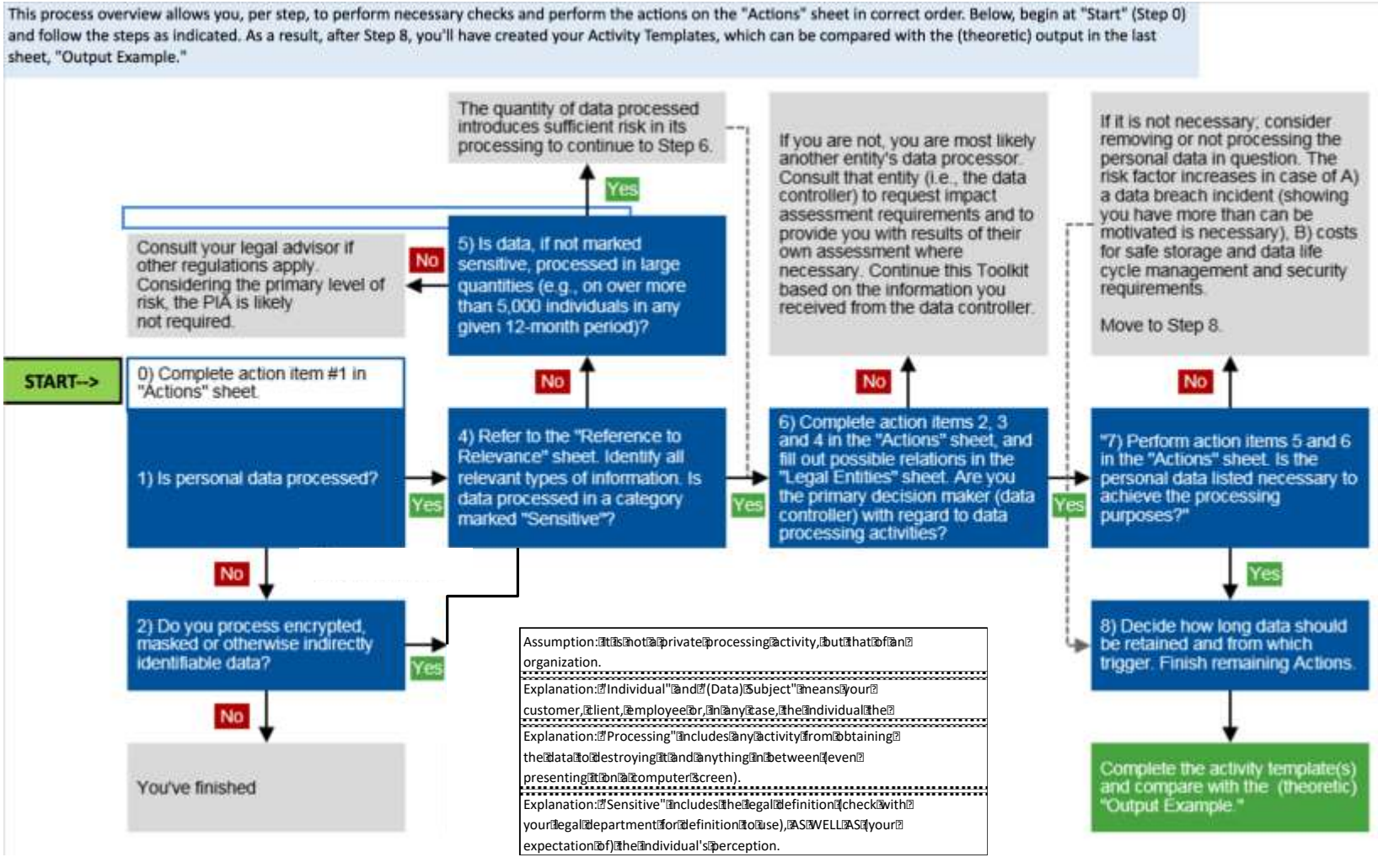
Catalog & Categorize

- Application Inventory created
  - Approx. 283 IEEE applications
  - Personal data is captured or processed in 157 applications
  - Taskforce led the effort
- Information Classification
  - Highly confidential
  - Confidential
  - Internal
  - Public
- Category
  - Processes data
  - Stores data
  - Both
  - Questionable

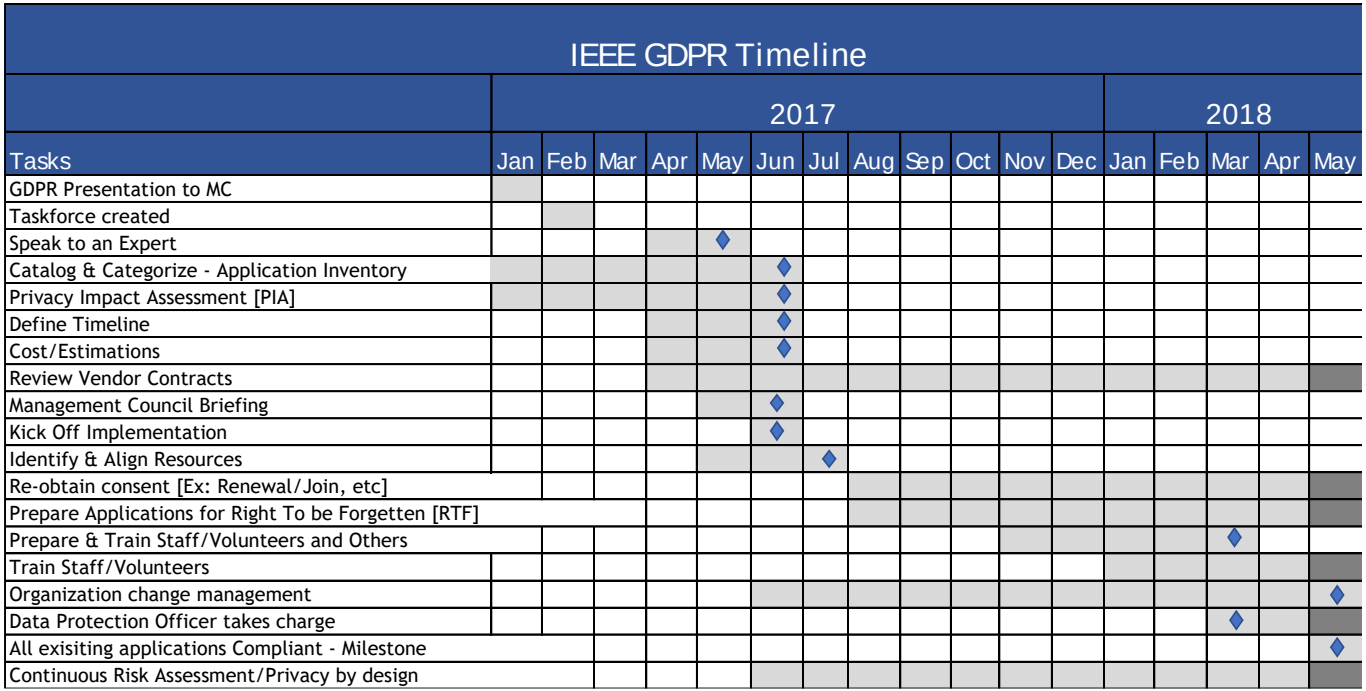
Privacy Impact Assessments

- What is a PIA?
- PIAs being created for all business processes
- Determine what changes are needed
  - Potentially eliminate certain processes
  - Refrain from collecting information that is not used/Data Minimization
  - Privacy by Design
- Document the need to store relevant data for legal or tax reasons

Privacy Impact Assessment Process Flow



Project Timeline



Privileged and Confidential Attorney Work Product

August 12, 2017

Region 8 Application

- GDPR applies to a large section of Region 8
- GDPR will impact Region 8 and IEEE activities
- Collaborative and committed cooperation will be necessary

Region 8 Actions

- Volunteers and staff must work together
- Need to bring awareness of GDPR
  - Communication plan
  - Compliance training module for data privacy and GDPR
- Develop and understand personal information that is downloaded and used
  - Collaborative development of an acceptable use policy
  - Areas of focus: SAMIEEE, Conferences
- Risk Mitigation

Questions

Priscilla Amalraj

Senior Director, Digital Center of Excellence

732 562 6553

j.prescila@ieee.org

Jonathan S. Wiggins

Senior Intellectual Property Attorney and Chief Privacy Officer

212 419 7544

j.s.wiggins@ieee.org

GDPR Taskforce: GDPRTaskforce@ieee.org