Professional

Information

Organization &

Technology

www.piothub.com

GDPR

Chuck Piotrowski
Founder & CEO
PIOT
chuck@piothub.com

PIOT

4/15/19	Agenda
1	Intro
2	Big Picture
3	Your Duty
4	To Do
5	Resources

What is PIOT

Hub dedicated to helping organizations create efficient, effective, and compliant information environments

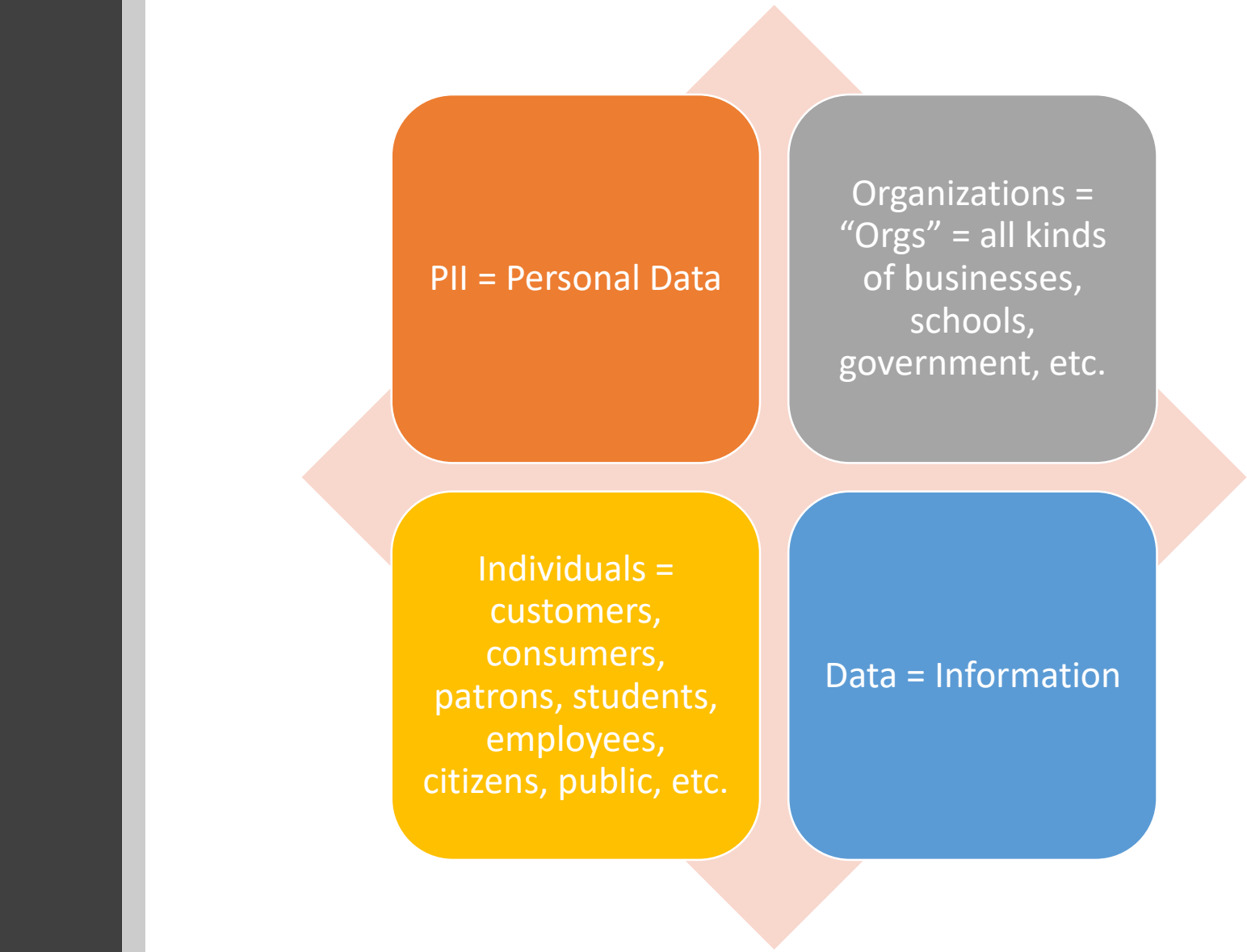
www.piothub.com

state government, multinational corporations, non-profits, public higher education, and highly regulated utilities

we love working with small businesses, start-ups, non-profits, and other organizations who just have a little bit of time to get stuff organized

PIOT

Vocabulary: Our talk will accept the following terms.



Big Picture

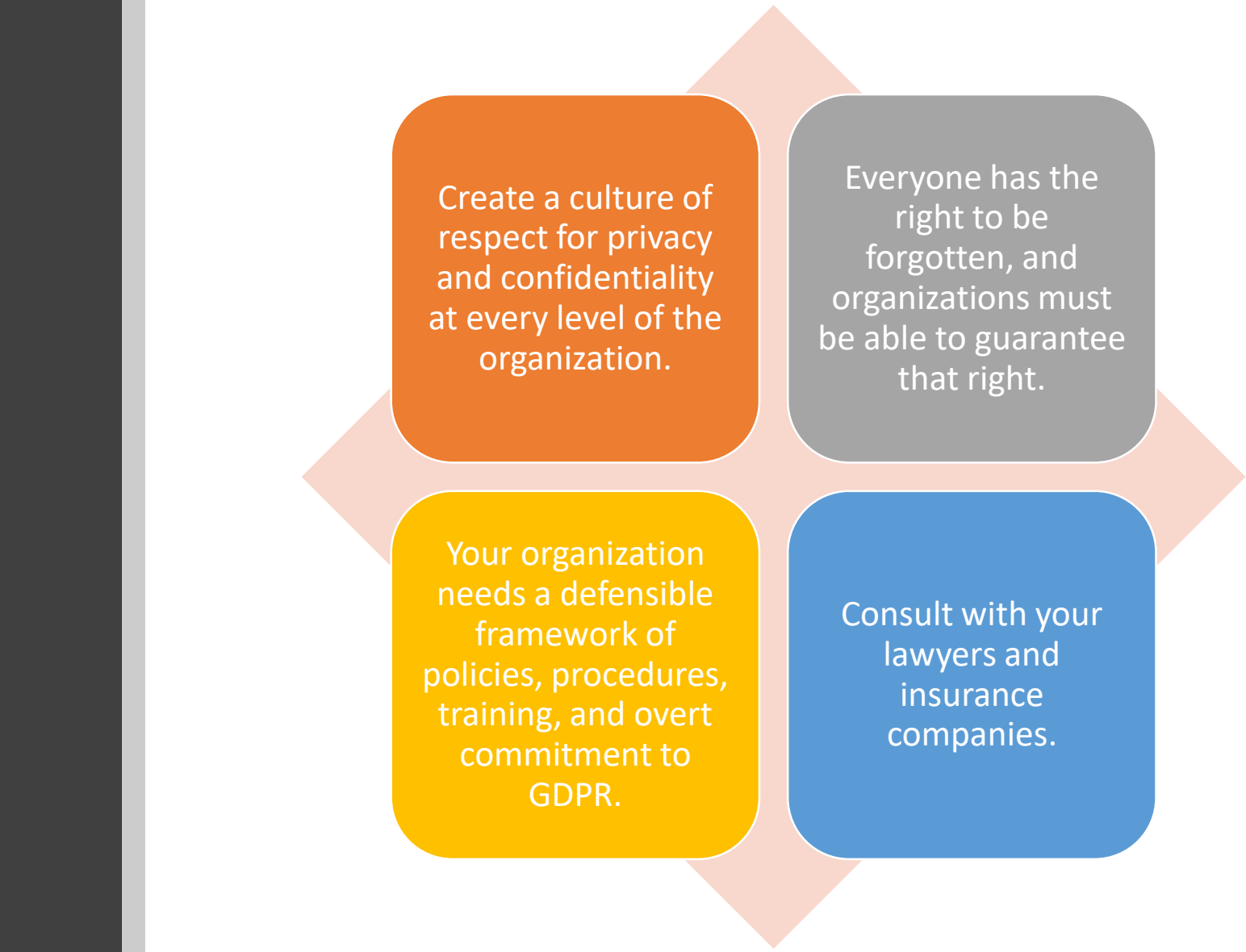

Create a culture of respect for privacy and confidentiality at every level of the organization.
Everyone has the right to be forgotten, and organizations must be able to guarantee that right.
Your organization needs a defensible framework of policies, procedures, training, and overt commitment to GDPR.
Consult with your lawyers and insurance companies.

Photo: https://eugdpr.org/

What is GDPR?

Protect European Union and European Economic Area from:

1. Mishandling of data
2. Inconsiderate and abusive use of personal information

Basic principle: Power to the People

- An organization can only work with the personal data of an individual if it is permitted by law or with the consent of that individual.
- Data about a person belongs to the person

Why GDPR?

Tradition of hundreds of years of government surveillance

The rights to private life and data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights (CFR) 2007

Supersedes the Data Protection Directive 95/46/EC

General recognition that businesses were collecting data to “target” individuals + poorly handling that data + being secretive with data

GDPR: General Issues

Protected: Personal Data

"any information relating to an identified or identifiable natural person."

Name and surname

Home address

Email address

Identification card number

Location data (for example the location data function on a mobile phone)

Internet Protocol (IP) address

Cookie ID

Advertising identifier of your phone

Data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Controllers & Processors

Controller: organization or individual who collects and uses personal data

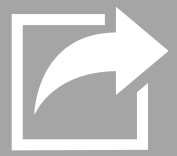
Processor: organization or individual who processes personal data on behalf of the controller

Processor could also be a cloud service provider storing personal data for clients

Organizations located outside of the EU doing business in EU states could be subject to the GDPR if those organizations process personal data from an EU state

Increased Territorial Scope (extraterritorial applicability)

All organizations processing the personal data of data subjects residing in the European Union, regardless of the organization's location.



Applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.

Processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.

Penalties

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater)

There is a tiered approach to fines

Apply to both controllers and processors

Clouds are not exempt from GDPR enforcement

Consent

Organizations must get consent from individuals - ‘Opt-In” – “explicit consent”

Consent language and terms must be easily understood - “Clear and plain” - “intelligible” - “easy”

Purpose and intent of collecting must be clearly stated

How to withdraw consent must be easy.

Data Breaches

Similar to many US state requirements

72 hour notification

Properly anonymized data may not trigger notification

Processors must notify customers and controllers "without undue delay."

Right to Access & Port

Individuals can ask organizations “where and for what purpose?”

Controller must provide a free copy of personal data in electronic format.

Processors must customers and controllers “without undue delay.”

Individuals can collect and give their data to another controller organization.

Data Erasure

- Right to be forgotten
- Organization must erase data
- Organization must stop dissemination.
- Halt 3rd parties from processing data
- Conditions: No longer needed by org or consent is withdrawn
- Orgs may refuse if public interest is greater than privacy

Data Protection Officers

Mandatory only for some controllers and processors

Organization core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale

Special categories of data: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or concerning a natural person's sex life or sexual orientation

Data relating to criminal convictions and offences

Your Duty

Organizational Awareness & Knowledge (OAK)

4/18/2019

Do you know…

- Where data is/are?
- Who has access?
- How long you can keep it?
- Which data is PII, sensitive, confidential?
- Who has accessed it?
- If it has been accessed by unauthorized personnel or outsiders (breach)?
- If it has been breached, what you must do?

To Do

Determine Organizational Responsibility

Bake into governance documents – Privacy Policy, Records Management Policy, Customer Service Policy, 3rd Party Contracts

Assign Responsibility and Accountability to a position – put it in the job descriptions

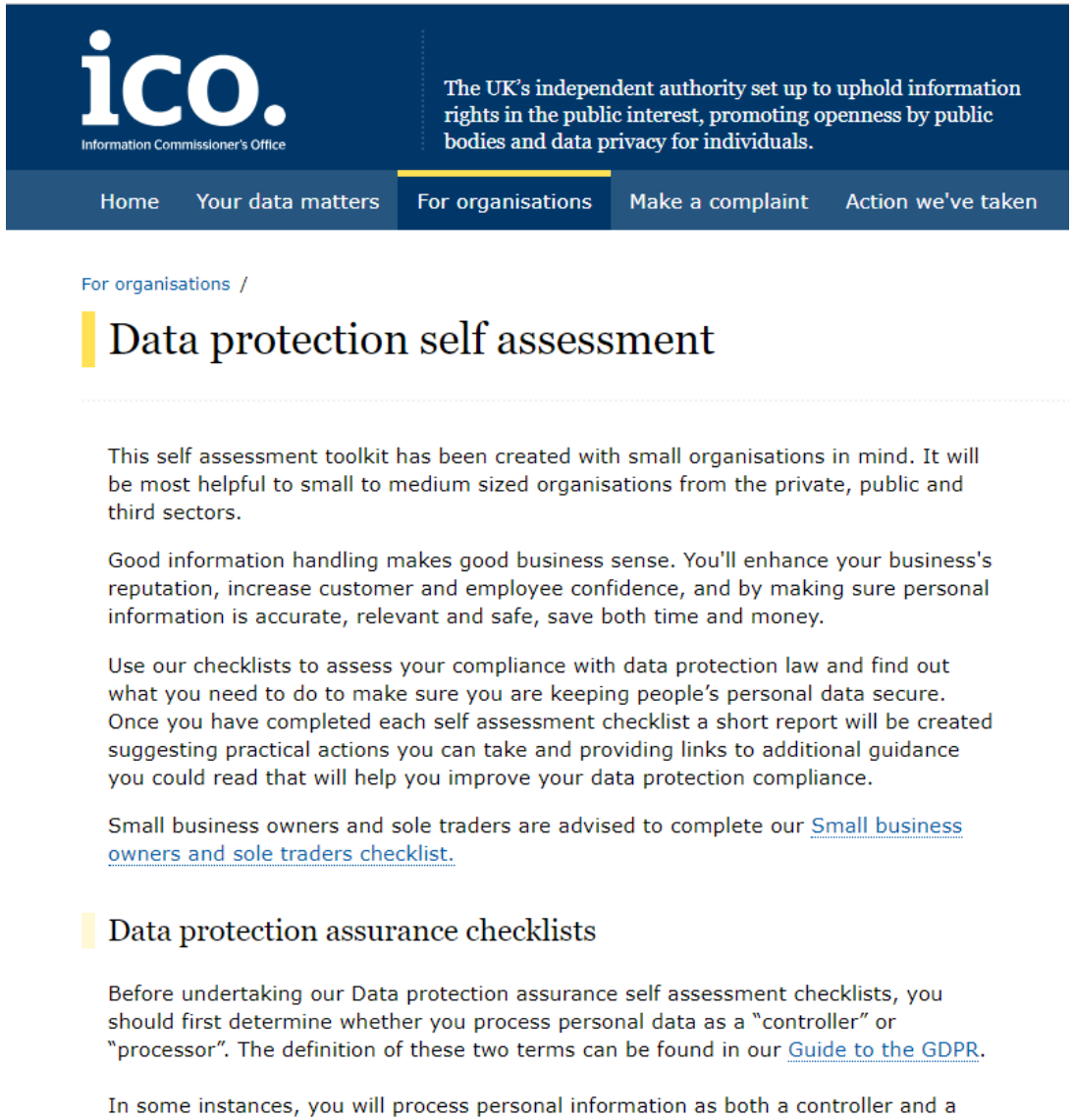
GDPR Team or Privacy team

Responsible Roles

- Executive Lead – Digital Protection Officer
- CEO
- CIO
- Audit
- Customer Service Manager
- CISO
- CPO – Chief Privacy Officer
- CAE – Chief Audit Executive

Assessment Inventory

- Know what you have, where you have it
- Inventory
- What are you collecting?
- Processes that collect PII
- Try the UK ICO Checklists
  - https://ico.org.uk/for-organisations/data-protection-self-assessment/



ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken

For organisations /

Data protection self assessment

This self assessment toolkit has been created with small organisations in mind. It will be most helpful to small to medium sized organisations from the private, public and third sectors.

Good information handling makes good business sense. You'll enhance your business's reputation, increase customer and employee confidence, and by making sure personal information is accurate, relevant and safe, save both time and money.

Use our checklists to assess your compliance with data protection law and find out what you need to do to make sure you are keeping people's personal data secure. Once you have completed each self assessment checklist a short report will be created suggesting practical actions you can take and providing links to additional guidance you could read that will help you improve your data protection compliance.

Small business owners and sole traders are advised to complete our Small business owners and sole traders checklist.

Data protection assurance checklists

Before undertaking our Data protection assurance self assessment checklists, you should first determine whether you process personal data as a "controller" or "processor". The definition of these two terms can be found in our Guide to the GDPR.

In some instances, you will process personal information as both a controller and a

Ask: Why?

When reviewing the inventory, ask why you are keeping that data.

Document the need and justification

Do you really, really need Personal Data?

!

Avoid data hording.

Review/Audit Processes Collecting & Interacting with PII

- Research reading room forms
- Online catalog registration
- Library card registration
- Mailing lists
- Event registration
- Orders – sales & delivery
- Website registrations
- Donation records
- Donor lists
- Deeds of Gift
- Vendor lists (Many DBA's in archive economy)
- HR
- Payroll
- Benefits
- Union
- Interns
- Student worker management
- Oral History authorizations
- Company culture events
  - Picnics, Retirements, Surprise Parties, telephone trees

Implement: Governance

Privacy Policy

Document processes

- Workflows
  - PII movement clearly identified
  - Storage (at rest) locations for PII
  - Role based ACLs

Ensure consistency in handling PII in all processes.

- Different data handling procedures within one organization for the same content is hard to defend.

Implement: Training & Education

Data handling procedures

Leverage org training

- New Hire
- Management

Partner with IT Security

Implement: Transparency & Clarity

Clarity in all statements

Explain why the organization is collecting info

- Example from the EU Internet Handbook: "This site uses cookies to offer you a better browsing experience. Learn more about how <name of organization> uses cookies and how to change your settings.“
- Example: Green Mountain Energy Company - https://www.greenmountainenergy.com/privacy-policy/

Hand out paper, if it is a physical event.

Implement: Youth Protection

Age documentation

You may have researchers under the age of 16, you will need approval from parents/guardians.

History day, Children events, Kid or Junior “zones” on the web

Hand out paper consent forms at physical events.

Implement: Retroactions

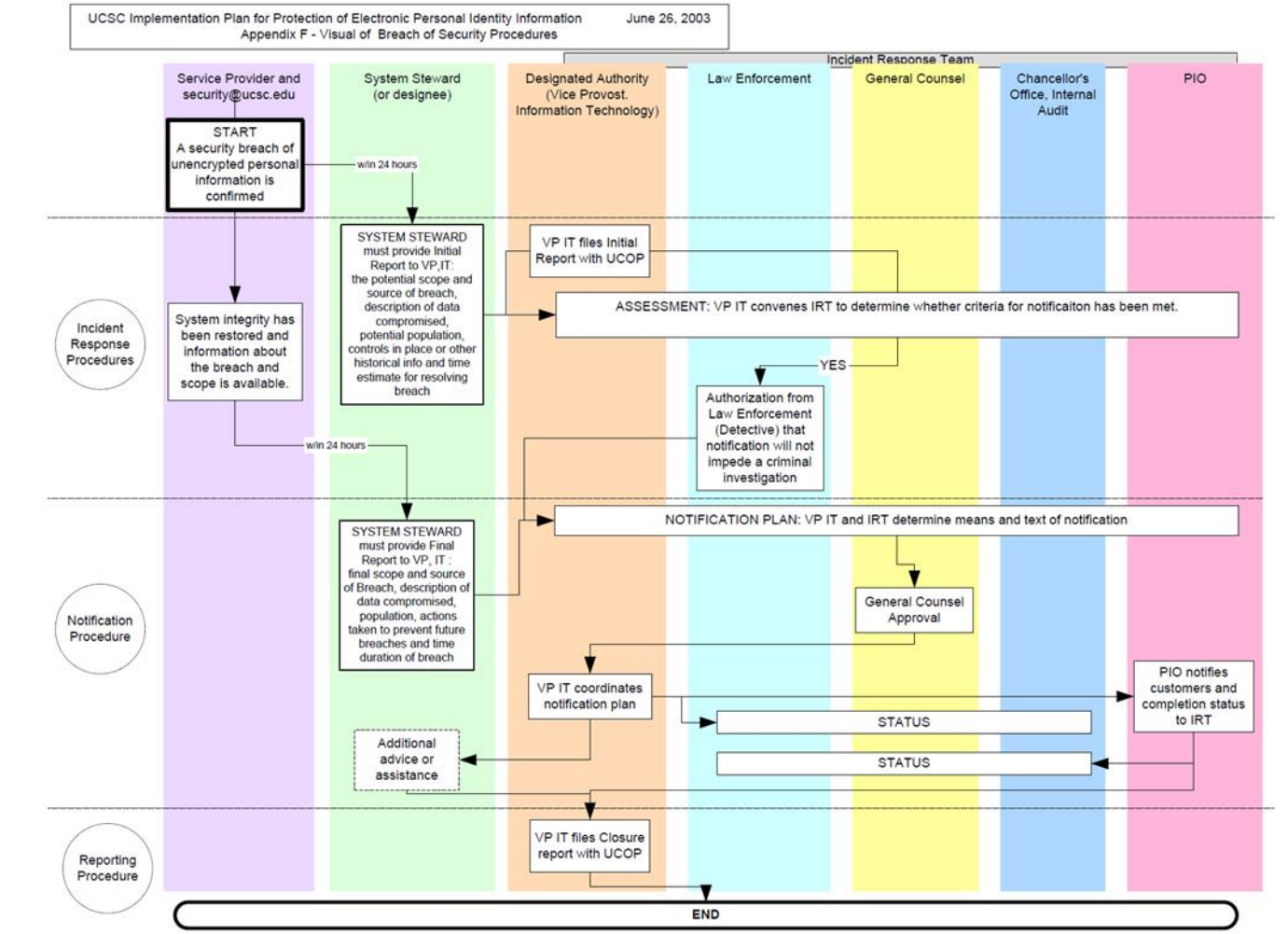
Data gathered Pre-GDPR

Reach out to individuals

Seek and respect opt-in

Treat all the same

Implement: Breach Notifications



Implement: Courteous & Deliberate Sharing/ Forgetfulness

Process for individuals to request their data.

Process for removing PII from everywhere

Customer friendly – clear – instructions for requests

Organizational direction for timeliness and responsiveness

Next?

GDPR as best practice

- Worldwide - Other governments are looking at it
- EU - The provisions of GDPR will be extended to electronic communications by a new e-Privacy Regulation, which is expected to come into effect later this year
- EU - These rules will govern how organizations can send out unsolicited marketing emails and text messages, will enable web users to set their cookie preferences on their browsers, and will stiffen up confidentiality rules for internet businesses.
- China last year introduced a slew of regulations on cybersecurity, data protection, and cross-border data transfer with distinctive GDPR-type features. California
- California Consumer Privacy Act of 2018, which takes effect in 2020, features opt-out clauses, transparency rules, and rights for customers to be forgotten similar to those contained in GDPR.
- US States looking at versions
- US Federal – Regulation in subject specific laws

Brexit

- The U.K. could potentially leave the EU without a formal set of agreements to govern how data on citizens is used between the two territories. If that happens, the U.K. will be covered by the 2018 Data Protection Act, which enshrines most of the provisions of GDPR into U.K. law.

Machine Learning and AI

- If it was so awesome, this slide content would be auto-generated with pertinent and actionable information!

Questions

- Zuck and more GDPR-type regs?

Resources

There are many organizations that can help with compliance. Feel free to Google. The next slide notes the resources that were used for making these slides.

Resources

- EU GDPR Portal: “Powered by Trunomi”
  - https://eugdpr.org/
- UK Information Commissioner’s Office
  - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
- European Union
  - https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm
- European Parliament
  - http://www.europarl.europa.eu/news/en/headlines/society/20180522STO04023/gdpr-is-in-effect-now-you-decide-on-your-digital-privacy
- Microsoft
  - https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-arc
- https://iaonline.theiia.org/2019/Pages/GDPRs-Global-Reach.aspx

-End-