Privacy Primer and General Data Protection Regulation (GDPR)

JIM KEESE

PRIVACY INTERNATIONAL, LLP

Agenda

Section 1 – Global Privacy

Overview of Personal Information
Global Privacy Landscape
Privacy Principles

Section 2 – GDPR Basics and Practices Areas

What is GDPR
Timing and Enforcement
Regulation Fundamentals

Section 3 – GDPR Requirements to Actions

Where to Start
Actions to Take
Short Term vs. Long Term Implementation

Section 4 – GDPR / InfoSec / Expectations

What is InfoSec's Role
GDPR Assessment - What to Expect

Global Privacy

PRIVACY INTERNATIONAL, LLP

Global Privacy

Personal Information

- Name, Address, Landline/Mobile Numbers
- Email Address, Nationality, Citizenship, Employee Data
- Financial Information, Health/Medical Data
- Criminal History

Notification, Consent and Choice

- Narrative of the Organizations' Purposes and Use
- Ability for the Individual to Consent to Types of Use
  - Presented and Recorded at Point of Collection
  - Ability to Change or Remove Consent (Opt-in vs. Opt-out)
- When Consent is not required

Global Privacy

Purpose and Use

- Organizations Can Only for Purposes Provided in the Notification
- Primary Use Typically Does Not Require Consent
- Secondary Use Typically Does Require Consent

Retail vs. Web vs. Mobile

- Practices for Notification and Consent Vary
- Acknowledgement Using “Click Buttons” or Reply Processes

Global Privacy

Access and Right to be Forgotten

- Enable Individual Rights to Access
- Removal (Deletion) of PI from Systems and Files

Data Protection

- Limit Access to Those Whom Have a Business Need
- Data Security Increases Based on Sensitivity

Classification and Retention

- Define Data Set by Sensitivity
- Define the Period of Time the Data should be Maintained

GDPR Basics & Practice Areas

PRIVACY INTERNATIONAL, LLP

GDPR Basics

European Committee's Goal - One Single Regulation for the EU

Replaces the EU 95/46 EC Directive

The Directive was a guideline or "direction" vs. GDPR is a regulation

Enforcement date – May 25, 2018

Potential fines of between 2-4% annual turnover

Structured to address current state technology, international data transfers

GDPR Principles

- Lawful basis
- Fair processing
- Specify Purposes
  - Limitation
- Adequate, relevant, not excessive
  - Minimization
- Accuracy
- Retention
- Rights of Individuals
- Appropriate Data Protection
- International Transfer Adequacy

GDPR Key Requirements

- Increased Individual Rights
- Access to Data
- Remedy from Supervisory Body/Court
- Compensation for Damage
- Compensation for Distress
- Rectification (NEW)
- Objection
- Right to be Forgotten (NEW)
- Data Portability (NEW)
- Restrict Processing (Put on Hold)
- Automated Decisions and Profiling

GDPR Basics

Individual's Rights

- Choice
- Access
- Right to be Forgotten
- Data Portability

Applies to Any Organization that Collects Personal Data from a European (EU) Resident or Citizen

GDPR Basics

Requirements Extend to Contractors, Vendors and Suppliers

- Accountability and Validation of Data Protection
- Contractual Requirements within Your Agreements

Compliance requirements

- Record Keeping
  - Access Requests and Actions
  - Choice Changes/Updates
  - Data Portability Requests
- Data Protection Impact Assessments

GDPR Basics

Applicability - Extra Territorial

- Based on Residency of Individuals
- Applies to Tendering of Goods or Services
- Monitoring of Behavior (Internet Tracking and Profiling)

Processing Personal Data

- Location Does Not Matter
- Applies to Personal Data When an Individual Can be Identified
- Any Format (digital, paper, audio, video etc.)
- Broad Scope Beyond Textual Data; Pictures, IP Address, Device IDs, Cookies, etc.)

Metrics, Measure and Certification of Compliance

GDPR Practice Areas

Assignment of a Data Protection Officer ("DPO")

- Reports to an Executive Officer
- Responsible for GDPR Compliance
- Independent, Role is Free of Organizational Objectives

Awareness

- Organizational, 3rd Parties and Executive Responsibilities

Data Inventory

- Identify and Document the Information an Organization Maintains

Privacy Notice

- Clear and Transparent on the Collection, Use and Processing

GDPR Practice Areas

Individual Rights

- Right to be forgotten, Access and Consent

Legal basis

- Document the basis for processing data, types of data processing and purposes

Data Breach

- Documented and Tested Incident Management Plan; Procedures, Detection and Reporting

Data Protection Impact Assessments

- Document the level of compliance for systems, databases, data stores, communications

GDPR Practice Areas

Data Classification and Retention

- Mapping of Data Flows
- Classification Based on Sensitivity
- Applying Retention Periods and Provide Evidence

Data Protection

- Periodic evaluation of 3rd party service providers, contractual terms, encryption, logging, etc.
- Data Protection Measures Based on Classification

International Data Transfers

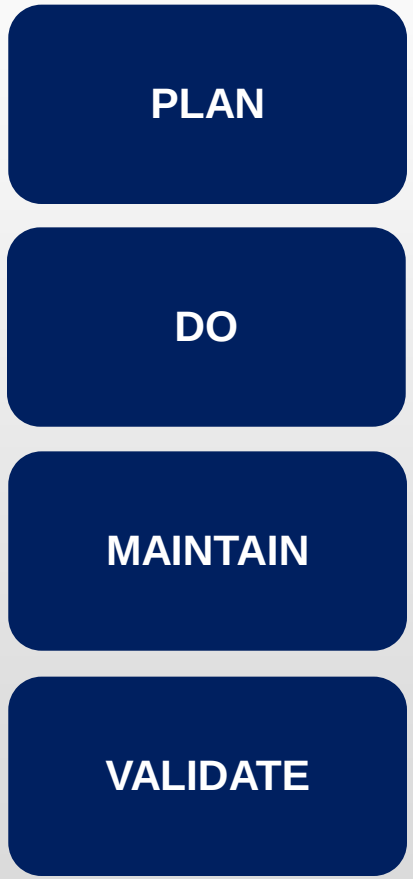
- Notification to the Lead Authority,
- Execution of Transfer Agreements (BCR's, Model Contracts, Privacy Shield (in Question with EU Authorities)

GDPR Requirements to Actions

PRIVACY INTERNATIONAL, LLP

Life Cycle Approach

1. Scope
2. Links to Business Areas
3. Terms and Definitions
4. Context of the Organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Enhancement



GDPR Requirements to Actions

PREPARE AND PLAN

- Involvement of Stakeholders from the Outset
  - Recommendations Include, Information Security, Compliance, Privacy, HR, Marketing, Sales, Legal, IT and Vendors
- Document Types of Data Collected from the Consumer, Customer, Employee or Client
- Identify the Data, Sources, Exemptions (i.e. HR data) and Storage Locations

DPO

- Secure your Data Protection Officer (DPO), ensure they are Independent and Reports to Executive Level

IDENTIFY

- Validate User Access, Role and Functionality (view only, extract, modify, etc.)
- Security Measures, encryption, intrusion detection, audit logs, etc.

GDPR Requirements to Actions

ASSESSMENT

- Complete Questionnaires to Enable Evaluation
- Identification of Gaps

DATA/PROCESS MAPPING

- Map Out the Data Flows and Processes
- Cross Border Transfer Means
- Storage Locations and Backup Sites/Systems

DOCUMENTATION

- Review Policies, Standards, Controls, Standard Operating Procedures
- Access, Correction, Right to be Forgotten and Data Portability Processes
- Data Breach Response Procedures

GDPR Requirements to Actions

ALIGNMENT

- Review External Privacy Statements, Notices
- Consents and Terms and Conditions, Alignment with Company Practices and Do Not Conflict

TRAINING

- Develop and Roll Out Training and Awareness

CONTRACTS

- Review Your Contractual Agreements with Vendors, Processors and Resource Providers

REPORTING

- Determine Frequency of Reporting Metrics and Recipients' within Executive Management

GDPR / InfoSec / Expectations

PRIVACY INTERNATIONAL, LLP

GDPR Key Areas for InfoSec

Develop a Data Protection Checklist for 3rd Parties (service providers, software, cloud..)

Evaluate and Document Level of Compliance

Assist in Documenting the Lifecycle and Infrastructure of Data Protection

Incident Management, Evaluate Your Current Process, Update and Test

- Reporting of Event/Incidents to the DPO is a Requirement
- DPO has Responsibility to Notify Lead DPA within 72 Hours of a Security Breach

Awareness, Incorporate GDPR Data Protection Requirements into InfoSec Training

- Complete Testing of Staff/Vendor Awareness such a "Phishing Exercises"

GDPR Compliance - What to Expect

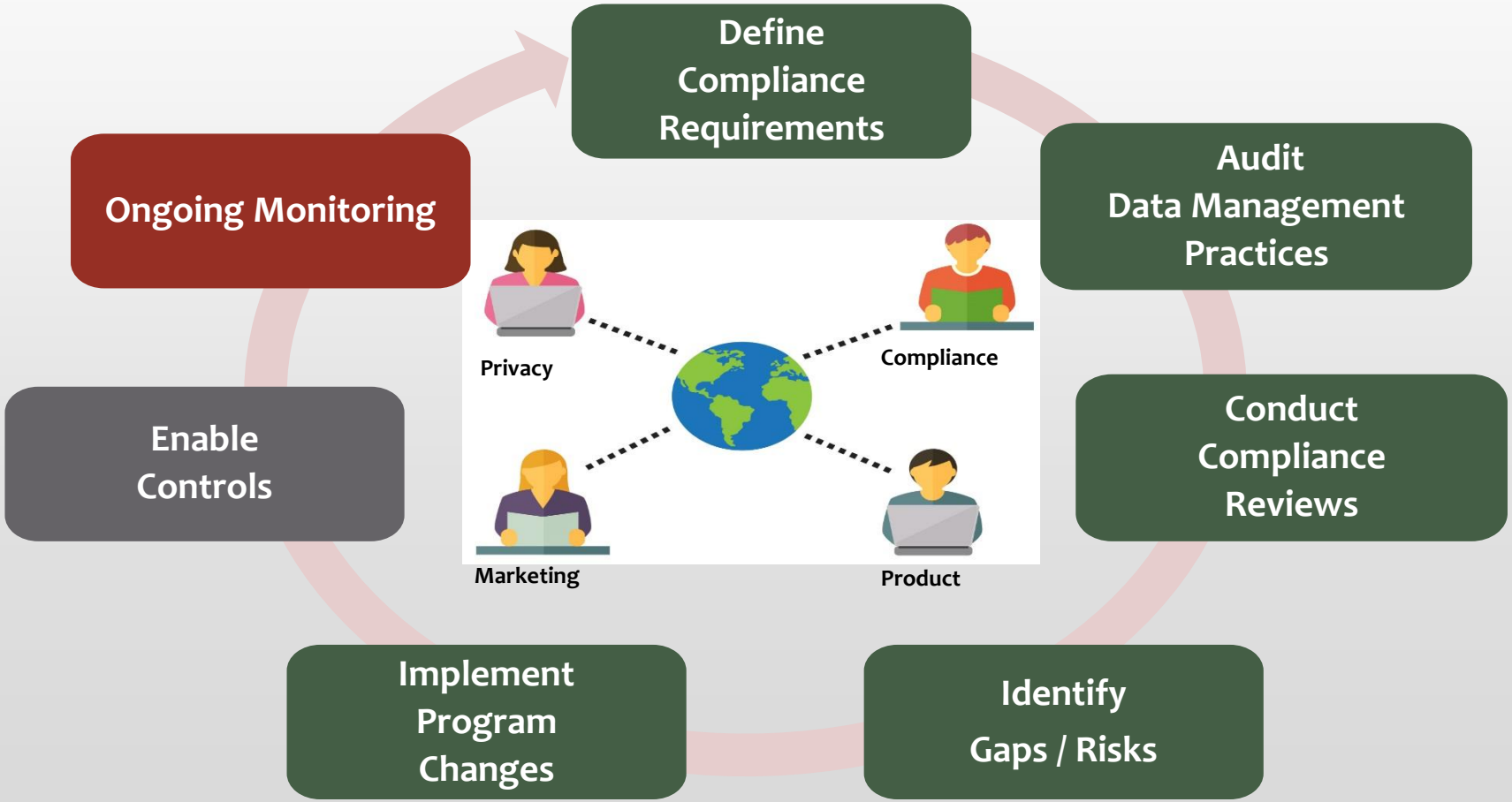
Privacy Risks that Should Be Evaluated

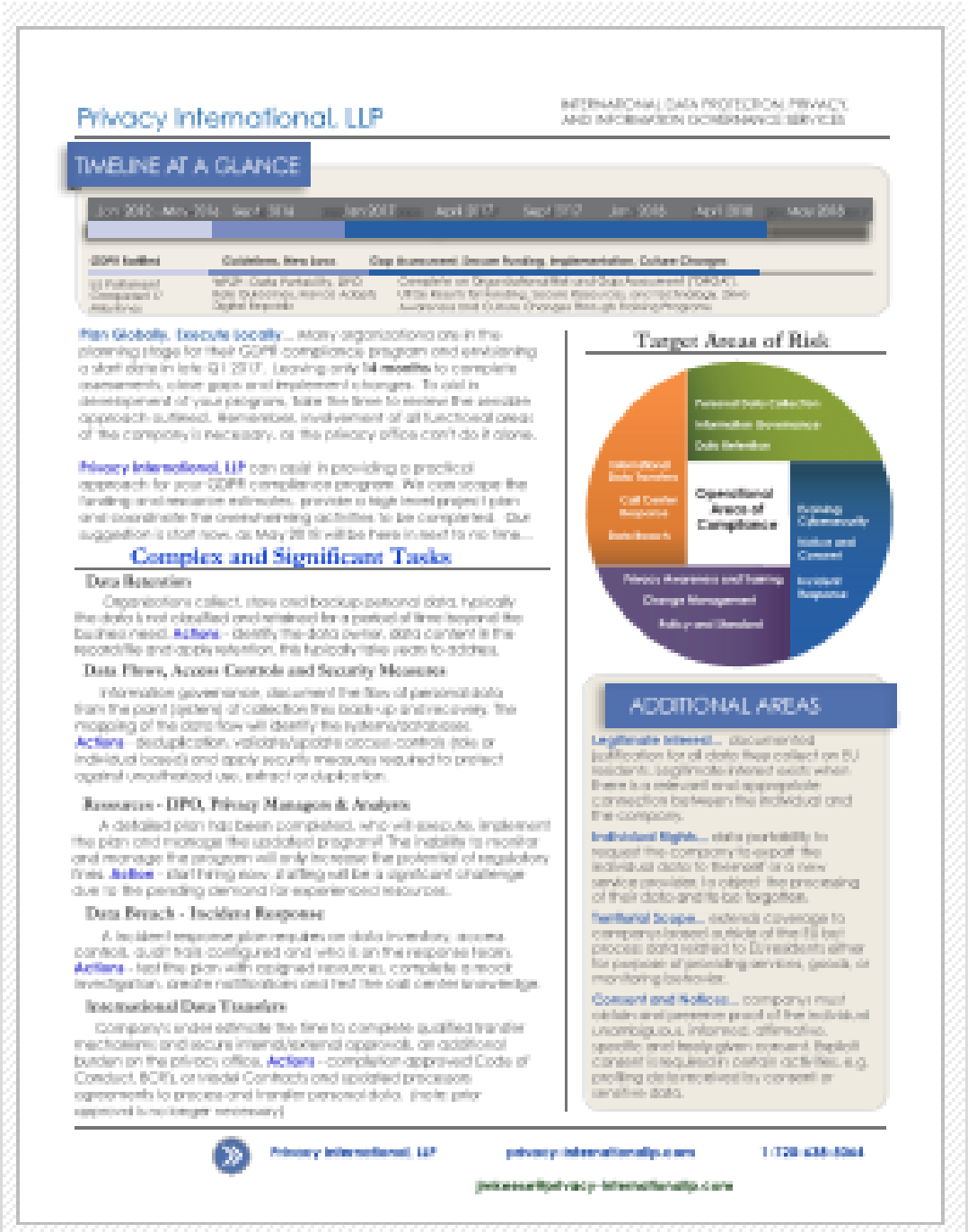
- EU National Laws may set up Additional Penalties (enforced audit, reprimand, criminal sanctions)
- Fines
- Increased Consumer Awareness
- Increased Activism
- Courts Increasing Findings for Individuals (courts as activists)

- Greater "Visibility" of Privacy in the Media
- Ethical Business Practices ("creepiness")
- Reputational Harm
- Decreased Consumer Trust
- Increased Board Awareness

Continual Improvement… Never Ends!

Assess, Remediate, & Operationalize --- Enterprise-wide





Privacy International, LLP

INTERNATIONAL DATA PROTECTION, PRIVACY AND INFORMATION GOVERNANCE SERVICES

TIMELINE AT A GLANCE

Jun 2012 · May 2016 · Sept 2016 · Jan 2017 · April 2017 · Sept 2017 · Jun 2018 · April 2018 · May 2018

GDPR Ratified · Guidelines, New Laws · Gap Assessment, Secure Funding, Implementation, Culture Changes

(1) Parliament Compliant to Regulation · WP29 Data Portability, DPO, Risk Guidelines, Impact Assess, Digital Economy · Complete an Organizational Risk and Gaps Assessment (ORGA) · Utilize Results for Funding, Secure Resources, and Set Priorities · Awareness and Culture Changes through Training Programs

Plan Globally, Execute Locally ... Many organizations are in the planning stage for their GDPR compliance program and constructing a short cycle in late Q1 2017. Leaving only **14 months** to complete assessments, close gaps and implement changes. To aid in development of your programs, take this time to review the possible approach outlined. Remember, involvement of all functional areas of the company is necessary, as the privacy office can't do it alone.

Privacy International, LLP can assist in providing a practical approach for your GDPR compliance programs. We can scope the funding and resource estimates, provide a high level project plan and coordinate the remaining activities to be completed. Our suggestion is start now, as May 25 th will be here in relation to no time...

Complex and Significant Tasks

Data Retention

Organizations collect, store and backup personal data, typically the data is not classified and retained for a period of time beyond the business need. **Actions** - identify the data owner, data content in the records file and apply retention, this typically takes years to address.

Data Flows, Access Controls and Security Measures

Information governance, document the flow of personal data from the point (system) of collection thru back-up and recovery. The mapping of the data flow will identify the systems/databases. **Actions** - deduplication, validate/update access controls (role or individual based) and apply security measures required to protect against unauthorized use, extract or duplication.

Resources - DPO, Privacy Managers & Analysts

A detailed plan has been completed, who will execute, implement the plan and manage the updated program? The inability to monitor and manage the program will only increase the potential of regulatory fines. **Action** - start hiring now, staffing will be a significant challenge due to the pending demand for experienced resources.

Data Breach - Incident Response

A incident response plan requires an data inventory, access control, audit trails configured and who is on the response team. **Actions** - test the plan with assigned resources, complete a mock investigation, create notifications and test the call center knowledge.

International Data Transfers

Company's under estimate the time to complete qualified transfer mechanisms and secure internal/external approvals, an additional burden on the privacy office. **Actions** - completion approved Code of Conduct, BCR's, or Model Contracts and specified processor agreements to process and transfer personal data. (note: prior approval is no longer necessary)

Target Areas of Risk

ADDITIONAL AREAS

Legitimate Interest... documented justification for all data they collect on EU residents. Legitimate interest exists when there is a relevant and appropriate connection between the individual and the company.

Individual Rights... data portability to request the company to export the individual data to themself or a new service provider, to object the processing of their data and to be forgotten.

Territorial Scope... extends coverage to companies based outside of the EU that process data related to EU residents either for purposes of providing services, goods, or monitoring behavior.

Consent and Notices... company's must maintain and demonstrate proof of the individual unambiguous, informed, affirmative, specific, level freely given consent. Explicit consent is required in certain activities, e.g. profiling or is received by consent or sensitive data.

Privacy International, LLP privacy-internationallp.com 1-720-638-5064

jmkeese@privacy-internationallp.com

Thank You

Contacts:

jmkeese@privacy-internationallp.com

1-720-638-5064

privacy-internationallp.com