GDPR is HERE!

Ryan Hogan
AppSec Consulting
Who owns PII?

In Europe PII about a data subject belongs to...

the data subject!
PII or Not PII: that is the question!

- Anonymous data
- Aggregated data
- Bank account number
- Biometrics (e.g. fingerprint, retinal scan)
- Birth date
- Cookies
- Criminal offenses and convictions
- Demographic information (zip code, city population, avg. income)
- Union membership
- Employee ID
- Ethnicity / Race / Citizenship
- IP addresses
- Mobile device ID
- Password
- Personal email address
- Personal Health Information (PHI)
- Phone #
- Physical address
- Picture
- Political affiliation
- Religious affiliation
- Sexual orientation
- SSN
- Drivers license #
- Title
- User ID / User name
- Work email address
- Philosophical beliefs
PII or Not PII: here are the answers!

**PII**
- Cookies
- Employee ID
- Picture
- User ID
- Email address
- Personal email address
- Password
- Bank account #
- Phone #
- Physical address
- User name
- Birth date
- Mobile device ID
- IP addresses

**Sensitive PII**
- Political affiliation
- Religious / Philosophical beliefs
- Sexual orientation
- Biometrics (i.e. Fingerprint, retinal scan)
- Health information
- Union membership
- Ethnicity / Race / Citizenship
- SSN
- Drivers license #
- Criminal offenses and convictions

**Not PII**
- Title
- Demographic information (zip code, city population, avg. income, # of children)
- Aggregated data
- Anonymous data / Pseudonymous data
Data Controller vs. Data Processor

Process = doing stuff with data - GDPR Art 4 (2)
Data Controller = determines means of processing GDPR Art 4 (7)
Data Processor = processes data on behalf of the controller GDPR Art 4 (8)
Timeline

Data Protection Directive (DPD)

General Data Protection Regulation (GDPR)

EU Safe Harbor

Swiss Safe Harbor

EU Privacy Shield

Swiss Privacy Shield

EPrivacy Directive

EPrivacy Regulation

Aren’t EU Privacy Shield and the GDPR the same thing?

- Privacy Shield is the replacement for Safe Harbor
- Provides legal mechanism to transfer PII data from the EU
- Complaint resolution 45 days
- Privacy Shield is based on the DPD – Not the GDPR
- Privacy Shield will likely get revised to align with the GDPR
- Most changes are not significant, so if you are Privacy Shield compliant you are 80-90% of the way towards being GDPR compliant
GDPR – No, it is not a new designer drug

What is GDPR?
• General Data Protection Regulation

When does it go into effect?
• May 25, 2018

Why should I care about it?
• Fines up to €20 million or 4% annual global turnover for violations of GDPR principles, rights, or transfer
• Fines up to €10 million or 2% annual global turnover for other violations including security breaches & no DPIA
So what's in GDPR that isn't in Privacy shield?

- Privacy notices
- Data Portability
- Data Protection Officers (DPO)
- Data Protection Impact Assessments (DPIA)
- Tried and tested Security Program
- Breach Notification
- Records
- Children
# GDPR Member State Variation

- Age for parental consent
- Processing PHI
- Processing Criminal offenses data
- Processing national ID #s
- Processing employee PII
- Data Protection Officer Required
Some GDPR Requirements

Notices
• Concise and easy to understand

Data Portability
• Machine readable, commonly structured form

Data Restriction
• Data Restriction is new right in GDPR – restriction rather than erasure
Data Protection Officer

SHOULD YOUR COMPANY APPOIN A DATA PROTECTION OFFICER (DPO) UNDER THE EU GDPR?

YES

- Do your core activities consist of processing which requires regular and systematic monitoring of individuals on a large scale?
  - Yes
    - Appoint a DPO
  - No
    - DPO not required by the GDPR (1)

- Do your core activities consist of processing which in itself special categories of data (1) on a large scale or about criminal convictions and offenses?
  - Yes
    - Appoint a DPO
  - No
    - DPO not required by the GDPR (1)

IS YOUR COMPANY SUBJECT TO THE EU GDPR?

- Yes
  - Your company based in the EU (1)
    - The processing relates either to the offering of goods or services to the data subjects in the EU or to the monitoring of their behaviour taking place in the EU
      - Yes
        - Your company subject to the GDPR, follow orange box!
      - No
        - Your company not subject to the GDPR, follow orange box!
  - No
    - Your company based outside the EU (1)
      - The processing relates neither to the offering of goods or services to the data subjects in the EU nor to the monitoring of their behaviour taking place in the EU
        - Yes
          - Your company subject to the GDPR, follow orange box!
        - No
          - Your company not subject to the GDPR, follow green box!

- NO
  - DPO not required (1)
    - Do your core activities consist of processing which requires regular and systematic monitoring of individuals on a large scale?
      - Yes
        - Appoint a DPO
      - No
        - DPO not required by the GDPR (1)
    - Do your core activities consist of processing which in itself special categories of data (1) on a large scale or about criminal convictions and offenses?
      - Yes
        - Appoint a DPO
      - No
        - DPO not required by the GDPR (1)
    - Is your company based in the EU (1)
      - Yes
        - Your company subject to the GDPR, follow orange box!
      - No
        - Your company not subject to the GDPR, follow green box!
    - Are you processing personal data (2)
      - Yes
        - Your company subject to the GDPR, follow orange box!
      - No
        - Your company not subject to the GDPR, follow green box!
DPIA and Dataflow

- Basically a risk assessment focused on data privacy risks
- To truly understand your risks you will likely need to do a data flow analysis (data inventory and data flow mapping)
Children

- What is a child?
- Understandable notices
Records

- Requires both controller and processor to keep records of processing activities
- I’d roll this into your customer and partner contracts so you don’t need to track a separate “record”
- Complaint resolution records (45 days)
EPrivacy Directive vs. the EPrivacy Regulation

How is the EPrivacy Regulation different from the EPrivacy Directive?

- **The EPrivacy Directive (EPD) = guidelines to member states**
  - Currently in place
  - Applies to PII over the Internet
  - Requires:
    - Security of services and the PII
    - Confidentiality of communications
    - Prior Opt-In consent for digital marketing
    - Location processed only if anonymized or with consent

- **The EPrivacy Regulation (EPR) = regulation that forces consistency**
  - Currently in draft
  - Draft requires:
    - Extends to electronic communications (not just telecom and ISPs)
    - Wiretapping requires consent
    - Metadata anonymized or deleted unless you have consent
    - Consent for cookies harmonized with the GDPR
EPrivacy Regulation and the GDPR

- Desired finalization and release by May 2018 to coincide with GDPR
  - I wouldn’t bet on it: trilogue on the e-Privacy Regulation Fall of 2018.
- Analytics OK under certain circumstances (aggregation, no 3rd parties, possible to object)
- Cookie Walls or banners – banned
- Clear notices with opt in consent
- Consent to specific purposes and providers
- Privacy by default on browsers
- Direct marketing – prior opt in consent only
Cookie compliance checking today

- Review your cookies, tags, and forms and get rid of any no longer needed.
Why Bother?

- EU Privacy Shield provides a legal mechanism for data transfer of EU PII data that is on firmer ground than Standard Contractual Clauses and not as limited as Binding Corporate Rules.
- EU Privacy Shield and GDPR Compliance are likely pre-requisites for regulated EU customers.
- Being prepared means you will have taken key steps to:
  - Avoid GDPR Fines
  - Address privacy questions from customers and prospects
  - Understand what contractual requirements around privacy you can make for customers and prospects
  - Understand how PII flows through your systems
**So what do I need to do?**

<table>
<thead>
<tr>
<th>Action</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compare requirements against your practices</td>
<td>EU Privacy Shield / GDPR / Cookie Gap Assessment</td>
</tr>
<tr>
<td>Determine legal mechanism for transfer</td>
<td>Privacy Shield, Standard Contractual Clauses, Binding Corporate Rules</td>
</tr>
<tr>
<td>Figure out who has what PII</td>
<td>Data Inventory / Vendor Analysis</td>
</tr>
<tr>
<td></td>
<td>Data Flow Mapping</td>
</tr>
<tr>
<td>Limit your exposure</td>
<td>Update your privacy notice(s)</td>
</tr>
<tr>
<td></td>
<td>Determine your basis for lawful processing</td>
</tr>
<tr>
<td></td>
<td>Data retention</td>
</tr>
<tr>
<td></td>
<td>Data Protection Addendums</td>
</tr>
<tr>
<td></td>
<td>Privacy training</td>
</tr>
<tr>
<td></td>
<td>Data Protection Impact Assessments?</td>
</tr>
<tr>
<td></td>
<td>Data Protection Officer?</td>
</tr>
<tr>
<td></td>
<td>Security Certifications?</td>
</tr>
<tr>
<td>Be ready to act</td>
<td>Access / Rectification / Portability</td>
</tr>
<tr>
<td></td>
<td>Deletion / Restriction / Retention</td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
</tr>
<tr>
<td></td>
<td>Lead DPA?</td>
</tr>
<tr>
<td></td>
<td>Tabletop tests?</td>
</tr>
</tbody>
</table>
Resources

IAPP

- Articles and analysis
- Certifications
- Conferences and Training
- Tools
  - Cookie Tool
  - Assessment tool

EU General Data Protection Regulation (GDPR) - An Implementation and Compliance Guide

This must-have guide details what you need to do to comply with the GDPR. It covers:
> the GDPR in terms you can understand;
> how to set out the obligations of data controllers and processors;
> what to do with international data transfers;
> data subject rights and consent;
> and much more.

What format do I need?
DPAs lend a hand

- ICO (United Kingdom)
  - Self Assessment tools
  - Blog Posts
  - Whitepapers
- DPC
  - Whitepaper
- CNIL
  - Toolkit with templates (in French)
Ain’t no party like the Article 29 Working Party!
The Party’s Over...
Other Service & Solutions

While we don’t like to brag, here are a few things we’re really good at:

**Strategic Consulting/Advisory**
Our team of Security Experts provide industry-leading Risk Assessment, Project Management, and InfoSec Program and Policy Development services for SOC 2, ISO, GDPR and Privacy. We also provide outsourced CISO and DPO Services.

**Security Testing**
We provide thorough assessments of all types of applications, networks, and infrastructure with guidance for improving your security posture.

**Compliance and PCI Services**
Gap assessment and audit services with a focus on real security. Our experienced staff can help you reach your compliance goals in a manner best suited to your unique environment.

**Training and Awareness**
We offer engaging and interactive security awareness and technical training, both online and instructor-led.
Thank You!

Ryan Hogan | GCIH, GCWN, GCFE, CRISC, CIPM, CIPP/E
Director, Strategic Advisory Services

M: 650.703.9830
rhogan@appsecconsulting.com
www.appsecconsulting.com