GDPR is Here! Now What?
KEEP CALM I AM NOT YOUR LAWYER
Who owns PII?

- In Europe PII about a data subject belongs to...
  - the data subject!
PII or Not PII: Here are the EU’s answers!

**PII**
- Cookies
- User / Employee ID
- Picture
- Location data
- Email address
- Preferences / Interests
- Purchase history
- Password
- Bank account #
- Phone #
- Physical address
- Resume / CV
- Birth date
- Mobile device ID
- Behavior / activity
- Friend /Family relationships
  - 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**
- Demographic information (zip code, city population, avg. income, # of children)
- Aggregated data
- Anonymized data
- Public data (i.e. property records)
  - Pseudo-Anonymized 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)
## EU Regulatory Timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Directive (DPD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Data Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulation (GDPR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Safe Harbor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swiss Safe Harbor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EU Privacy Shield</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swiss Privacy Shield</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPrivacy Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPrivacy Regulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>California Consumer Privacy Act (CCPA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Secure360.org | #SEC360
GDPR vs other Privacy laws
GDPR – No, it is not a new designer drug

• What is GDPR?
  • General Data Protection Regulation

• When did 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
CCPA – It’s not about accountants

- What is CCPA?
  - CA Consumer Privacy Act
- When does it go into effect?
  - Effective January 1, 2020; Enforced July 1, 2020
- Why should I care about it?
  - Civil penalties (fines) of up to $7,500 for each “intentional violation”
  - Private actions of $100-$750 per consumer per incident
  - Imagine Equifax breach happens after July 2020
    - 143M * $100 = $14.3 B
    - 143M * $750 = $107.25B
## GDPR vs the CCPA

### Similarities
- Notice
- Breach notification requirements
- SARs must be free

<table>
<thead>
<tr>
<th>GDPR</th>
<th>CCPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforced by Supervisory Authorities</td>
<td>Enforced by CA Attorney General</td>
</tr>
<tr>
<td>Applies to anyone in the EU</td>
<td>Applies to CA “consumers”</td>
</tr>
<tr>
<td>Applies to individuals</td>
<td>Applies to individuals and households</td>
</tr>
<tr>
<td>Individuals have rights of access, portability, rectification, deletion, restriction, object</td>
<td>Individuals have rights of inform, access, portability, deletion, object, non-discrimination</td>
</tr>
<tr>
<td>Consumers opt-in to selling of their PII</td>
<td>Consumer opt out of selling of their PII</td>
</tr>
<tr>
<td>30 days to address SARs</td>
<td>45 days to address SARs</td>
</tr>
</tbody>
</table>

- Private right of action (lawsuits)
- Employee training
GDPR vs. EU Privacy Shield

- Privacy Shield is the replacement for Safe Harbor
- Provides a legal mechanism to transfer PII data from the EU
- Complaint resolution required within 45 days
- Privacy Shield is based on the DPD - not the GDPR
- Privacy Shield will likely get revised to align with the GDPR - or be revoked

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
EPrivacy Directive vs. the EPrivacy Regulation

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 with consent

VS.

EPrivacy Regulation (EPR) = Regulation that forces consistency
- Currently in draft
- Requires:
  - Coverage of all kinds of electronic communication (not just telecom)
  - Wiretapping requires consent
  - Metadata anonymized or deleted unless you have consent
  - Consent for cookies w/GDPR
What about GDPR Certifications and Codes of Conduct?

CERTIFICATE BULLSHIT

EVERYWHERE
Fines, Action & Fear - Oh My!
The UK’s ICO is one of the better funded and run Data Protection Authorities

- Not afraid to fine
  - Security and services and the PII
  - Confidentiality of communications
  - Prior Opt In consent for digital marketing
  - Location processed only if anonymized or with consent
- Not afraid to go after government agencies or nonprofits
• Egregious violations - not whoopsies
  • Equifax Ltd. £500,000 fine for failing to protect the PII of 15 million UK citizens
  • A company behind 99.5 million nuisance calls was been fined £400,000 by the Information Commissioner’s Office
  • Between 2011 and 2015 Great Ormond Street Hospital Children’s Charity shared 910,283 records and was fined £11,000
  • Miss-sold Products UK Ltd fined £350,000 after they failed to ensure that marketing calls were only made to individuals who had consented to receive marketing
• In roughly a third of cases the companies were given an “Enforcement Notice” before a fine
• GDPR lawsuits - private right of action not really used yet
Notable GDPR Fines to date:

**Summer 2019**
DPC (Ireland) and ICO (UK) are expected to announce some “notable fines”

**March, 2019**
Poland Data Processor €220,00
A data processor was fined because they scraped the internet for public contacts and conducted commercial outreach to over 90,000 people, 12,000 of which objected to unauthorized use of their data.

Denmark Taxi Company 1.2M DK (€160,714)
As a result of a random audit, the company was found to have over 9M personal records the company had stored but did not need to. The fine came as a result of a failure to delete this unused contact information.

**January, 2019**
France Google €50M
Google was fined from France’s data regulator, citing a lack of transparency and consent in advertising personalization, including a pre-checked option to personalize ads.

**December, 2018**
Portugal Hospital €400,000
Staff at the hospital used bogus accounts to access patient records.
Creating & Executing An Ongoing Privacy Program
# 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, 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 policy</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, deletion, restriction, retention, incident response, Lead DPA, tabletop tests</td>
</tr>
</tbody>
</table>
## Actions & Ongoing Activities

<table>
<thead>
<tr>
<th>Notification</th>
<th>EU Privacy Shield</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Required language for Employee &amp; Public Privacy Policies</td>
<td>• Concise and easy to understand notice</td>
</tr>
<tr>
<td></td>
<td>• Cookie Policy</td>
<td>• Privacy included in Employee Handbook</td>
</tr>
<tr>
<td>Choice</td>
<td>• Gather consent from customers and EU employees</td>
<td>• Consent for profiling</td>
</tr>
<tr>
<td></td>
<td>• Cookie Opt Out</td>
<td>• Consent for direct marketing</td>
</tr>
<tr>
<td>Data transfers to 3rd parties</td>
<td>• Create contract addendums</td>
<td>• Implement contract addendums</td>
</tr>
<tr>
<td></td>
<td>• Vendor due diligence process</td>
<td>• Vendor due diligence implementation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Records requirements</td>
</tr>
</tbody>
</table>
# Actions & Ongoing Activities

<table>
<thead>
<tr>
<th>Security</th>
<th>EU Privacy Shield</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Breach Response procedures</td>
<td>• Breach Response procedures</td>
</tr>
<tr>
<td></td>
<td>• Data Protection Impact Assessment</td>
<td>• Data Protection Impact Assessment</td>
</tr>
<tr>
<td></td>
<td>• Privacy training</td>
<td>• Privacy training</td>
</tr>
<tr>
<td></td>
<td>• Privacy documentation creation</td>
<td>• Data Protection Officer</td>
</tr>
<tr>
<td>Data Integrity &amp; Purpose Limitation</td>
<td>• Data Inventory</td>
<td>• Data Inventory</td>
</tr>
<tr>
<td></td>
<td>• Data Flows</td>
<td>• Data Flows</td>
</tr>
<tr>
<td></td>
<td>• Data Retention Policy</td>
<td>• Data Retention Policy</td>
</tr>
<tr>
<td></td>
<td>• Monitor Public Data Usage</td>
<td>• EU Representative</td>
</tr>
<tr>
<td>Access Requests</td>
<td>• Subject Access Request (SAR) Procedures</td>
<td>• Data Portability</td>
</tr>
<tr>
<td></td>
<td>• Independent Recourse Mechanism</td>
<td>• Subject Access Request (SAR) Automation</td>
</tr>
<tr>
<td></td>
<td>• Tabletop Exercise</td>
<td>• Tabletop Exercise</td>
</tr>
</tbody>
</table>

Secure360.org | #SEC360
How To Prioritize All Those Actions

- **Public facing GDPR compliance**
  - Privacy notice
  - Subprocessors
  - Cookie banners
  - DPO/EU representative

- **Complaints**
  - Prevention & Privacy Shield
  - Complaint process/procedures
  - Tabletop tests

- **Security Incidents**
  - Prevention and Appropriate Security
  - Procedures and tabletop tests
  - Notification

- **DPAs & Vendor Security**
  - Volume
  - Sensitivity
Why Bother?

• GDPR Compliance is a likely prerequisite for EU customers
  • Maybe Privacy Shield too
• Having a legal mechanism for EU PII data transfer will help keep you out of trouble (Standard Contractual Clauses, EU Privacy Shield, BCRs)
• Being prepared means you will have taken key steps to:
  • Avoid GDPR Fines
  • Increase customer trust
  • Develop a comprehensive privacy program that can be updated to reflect additional requirements for other jurisdictions
  • 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
Resources

IAPP

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

Consultants and Law firms
AppSec Consulting anyone?
DPAs lend a hand

ICO (United Kingdom)
- Self Assessment tools
- Blog Posts
- Whitepapers

DPC
- Whitepaper

CNIL
- Toolkit & templates (some only in French)
FAQs and Guidelines
I found these FAQs useful for GDPR clarifications:
• FAQ Lead Supervisory Authority
• FAQ DPOs
• FAQ Data Portability
These guidelines are a bit more dense, but can be useful if you are wrestling with questions not covered by the FAQs above.
• Lead Supervisory Authority Guidelines
• Data Portability Guidelines
• DPO Guidelines
• DPIA Guidelines
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.

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

**Certification Preparation and PCI Services**
SOC 2, ISO 27001 and PCI preparation and assessment services with a focus on real security. Our experienced staff can help you reach your certification and 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
rhogan@appsecconsulting.com
650-703-9830