



DrupalCon
NASHVILLE 2018

Think Your Website is GDPR Compliant?

Think Again!

April 10, 2018

Join Us for Contribution Sprints

Friday, April 13, 2018

**Mentored
Core sprint**

9:00-12:00
Room: Stolz 2

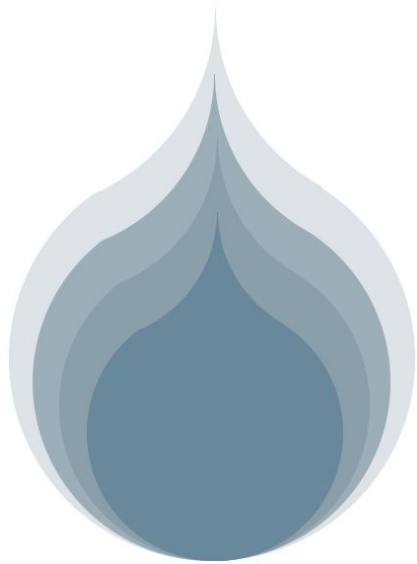
**First time
sprinter workshop**

9:00-12:00
Room: Stolz 2

**General
sprint**

9:00-12:00
Room: Stolz 2

#drupalsprint



DECOUPLED DRUPAL DAYS 2018

New York City

August 17–19, 2018

Drupal. JavaScript. Future.

Keynotes. Sessions. Sprints.

A different kind of Drupal conference.

Mark your calendar and prep your proposal!
More details soon.

Today's Team



Dawn Aly
VP, Digital Strategy
Mediacurrent
@dawnashleealy



Mark Shropshire
Open Source Security Lead
Mediacurrent
@shrop

Disclaimers

1. We are not lawyers.
2. This session is not a replacement for legal council.

Today's Agenda

- I. Guiding Principles of the GDPR
- II. Creating a Positive PX
- III. Security by Design
- IV. Advanced Marketing Strategies
in a Post GDPR World
- V. Creating an Action Plan
(not a Freak-Out Plan)

Guiding Principles of the GDPR

GDPR (General Data Protection Regulation)

What is GDPR?

GDPR (General Data Protection Regulation), adopted by the the European Union Parliament April 27, 2016, intends to give individuals in the EU the ability to control their personal data. International businesses will benefit by having simpler clarity around user privacy related regulations, leading to consistent implementations.

The GDPR become enforceable on May 25th, 2018 and replaces the 1995 Data Protection Directive.

Who is at Risk for Compliance?

Anyone who can say yes to at least one of the following:

- Do you have a website with international traffic?
- Do you use a CRM or Marketing Automation platform?
- Does your site have an analytics platform like Google Analytics?
- Does your website use cookies?
- Does your website collect personal information? Anything from a store or a contact form counts!
- Can users log in to your website?

A large crowd of people is seen from a low angle, looking up at a ceiling where a massive amount of confetti is falling. The confetti consists of many small, rectangular pieces of paper in various colors, including blue, white, and gold. The scene is illuminated by blue stage lights, creating a vibrant and celebratory atmosphere. In the upper right corner, a portion of a yellow metal truss structure is visible, with a bright blue light fixture attached to it. The overall composition is dynamic and captures a moment of high energy and excitement.

Yep. Pretty much everyone.

The GDPR is not just an IT Discussion

89%

Believe their competitive advantage will be based on the **customer experience**

85%

Percentage of relationships consumers will manage **without talking to a human by 2020**

43%

of cyber attacks targeted small businesses in 2015

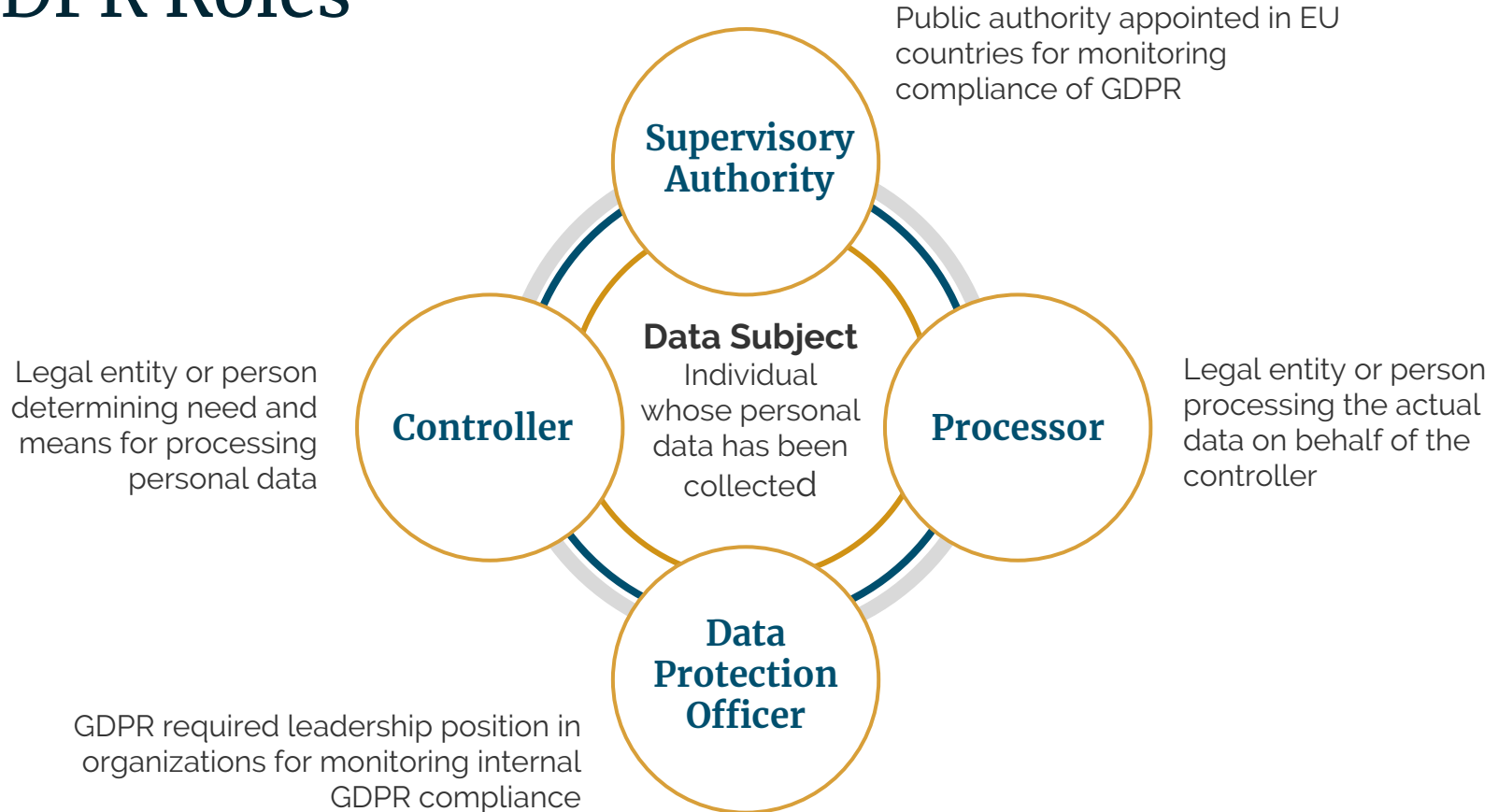
\$3.8 million

cost of a data breach for the **average company**

\$150 million

anticipated increase of data breach costs by 2020

GDPR Roles



User Rights and Requirements Overview



Breach Notification



Right to Access



Right to Erasure



Data Portability



Privacy by Design



Data Protection Officers

Breach Notification

- 72-hour supervisory authority notification requirement
- Notification not required if risk to the rights and freedoms of the individuals unlikely
- Individuals must be notified if they are impacted
- Notifications may not be required if the organization utilizes technical protections for personal data such as encryption



Right to Access

- Data Subjects have the right to access the personal data an organization is maintaining on them
- They have the right to request a copy of their personal data
- They have the right to know how their personal data is being processed, shared, and originally acquired



Right to Erasure (Right to be Forgotten)

- Data Subjects have the right to request their personal data be erased on a number of grounds:
 - Personal data use no longer necessary
 - Compliance of legal requirement
 - Illegal processing of data



Data Portability

- Data Subjects have the right to transfer personal data from one organization to another
- The organization holding the data cannot restrict or deny export of personal data
- Data must be presented in a structured manner with a commonly used electronic standard format
- Does not include data sufficiently anonymized



Privacy by Design

- Data protection and privacy should be designed and implemented into all systems and processes throughout the project life cycle
- Privacy by default stance to ensure that only data absolutely necessary for providing service is collected
- Personal data should only be retained for a time period deemed absolutely necessary to providing service



Data Protection Officers

- Similar role to corporate compliance officers
- Should have expert knowledge of data protection laws and practices to ensure regulatory compliance
- Required for public authorities processing personal data
- Also required for private sector organizations whose core operations involve monitoring of individuals




Key Challenges Ahead

- Implementation requirements are vague and often require interpretation
- Compliance and continued process improvements will come at a cost to organizations

Fines up to 20 million EUR or 4% of annual global turnover for noncompliance

Creating a Positive PX

PX (Privacy Experience)

A hand holding a smartphone, with the screen displaying a colorful bokeh pattern. The background is dark with many out-of-focus, colorful light spots in shades of purple, blue, green, orange, and pink. The text is overlaid on the right side of the image.

Data + Privacy
doesn't have to
be scary.

Universal PX Principles

- Always be transparent with users
- Use easy to understand language / no “lawyer speak”
- Consent must be given and not assumed
- Protect user data
- Don't collect more than absolutely necessary
- User must have the right to be forgotten
- Follow security and privacy by design methodologies



PII (Personally Identifiable Information) Examples

- Full name
- Face
- Home address
- Email address
- National identification number
- Passport number
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Do's

Don'ts

Data Collection

- Know what you collect
- Only retain for as long as you need
- Protect data with encryption
- Audit and log

- Collect any PII that you don't absolutely need
- Allow anyone or system access to data who doesn't have legitimate reason for processing

Transparency

- Have clear privacy policies
- Let users know how you use data and why
- Give users the right to decide how and when data is processed and shared
- Explain things in easy to understand language

- Hide who you share data with and why you share it with them
- Force users to opt-out (opt-in should be the pattern)
- Create hard to read privacy policies and other documents related to data privacy
- Rely on blanket consents

Data Portability

- Allow users control over their data including:
 - Exporting data
 - Deleting data
 - Seeing the details of their stored data

- Make it hard for users to export data in a standard format that is usable for imports to other systems and services
- Delay processing user request for deletion, export, or reporting

Security by Design

No waiting till launch time!

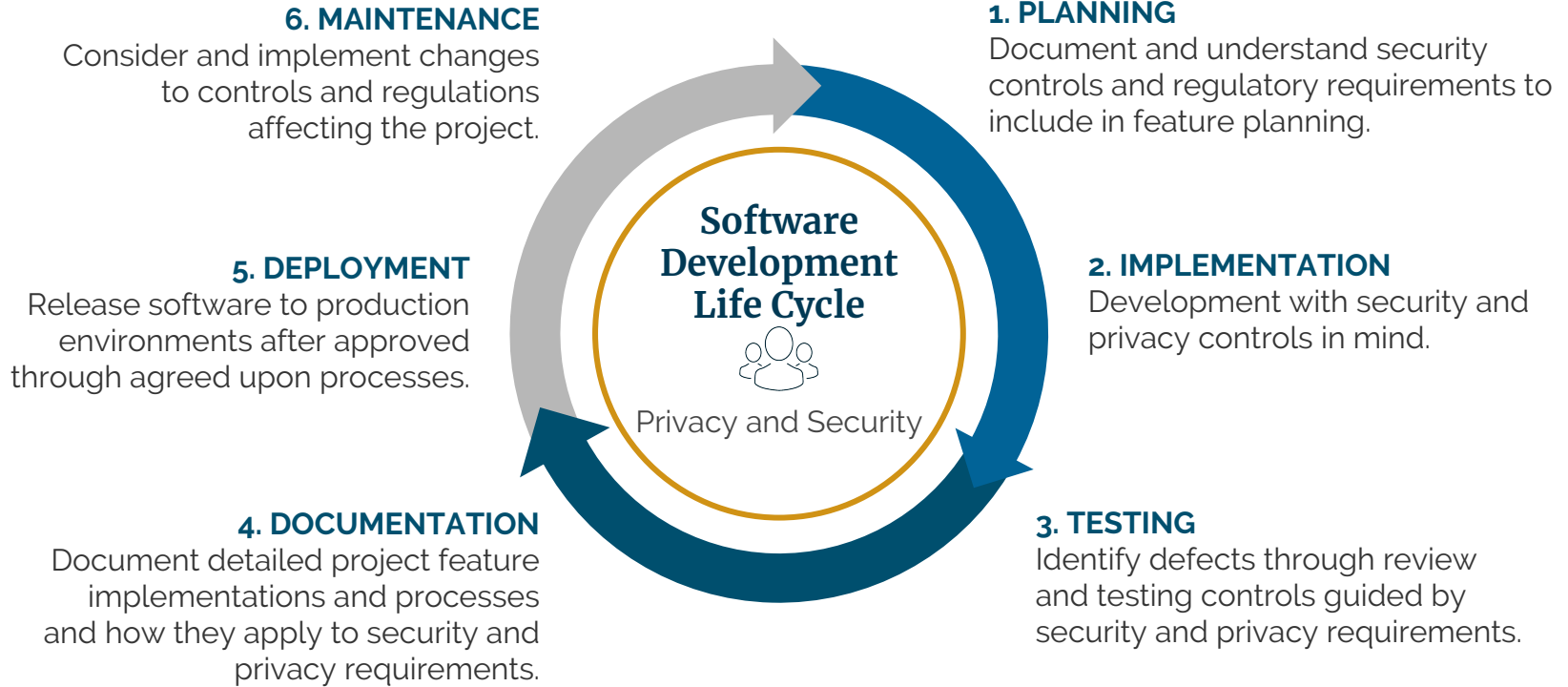
Secure by Design

Secure by design, in software engineering, means that the software has been designed from the ground up to be secure. Malicious practices are taken for granted and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input.

https://en.wikipedia.org/wiki/Secure_by_design



Privacy and Security SDLC



Security and Privacy Principles

- Limit attack surface
- Keep solutions simple
- Encrypt PII (Personally Identifiable Information)
- Know your regulatory requirements: FERPA, GDPR, HIPAA, PCI DSS, CAN SPAM etc.
- Write policies and procedures and then follow them
- Automate auditing and compliance processes
- Log events and transactions



One encryption key
per user

Delete key and
user is forgotten

Advanced Marketing Strategies

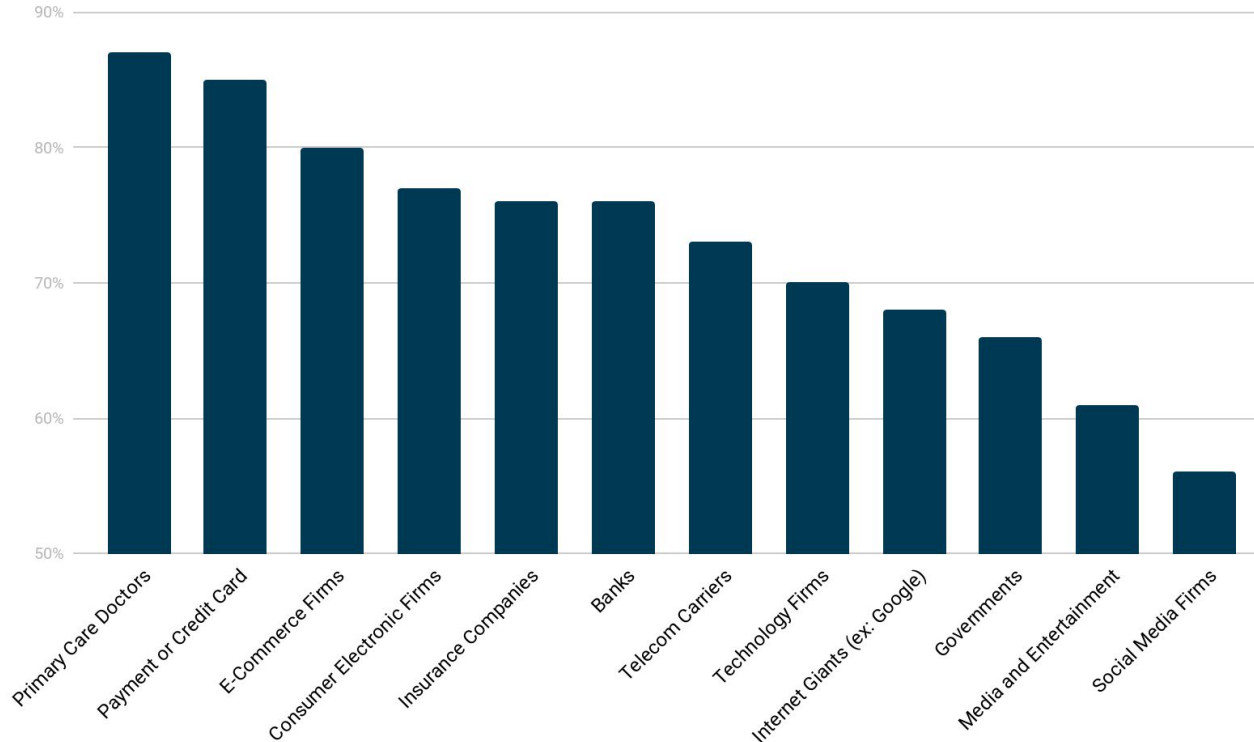
In a Post GDPR World

Make **Trust** Your
Competitive
Advantage

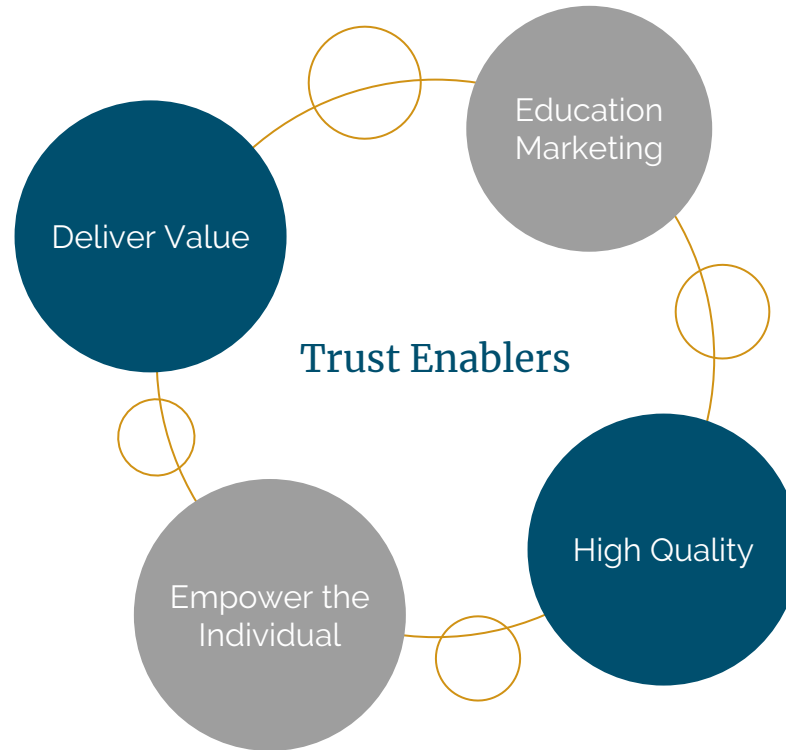
94%

of customers are likely
to be more loyal to
transparent brands

Level of Trust by Industry



Building Trust with Marketing



Big Data *May Not Be So Big*

and definitely comes with
bigger responsibility

GDPR Benefits to Data

- Improved data quality because it's submitted by the people it describes
- Potential reduction in data cleansing costs
- Marketing strategies will be in-line with customer desires vs marketers assuming what they want



Marketing Automation and CRM

- Be able to prove you have consent- even on past opt-ins
- Consent for one campaign doesn't mean consent for all
- Talk with your Marketing Automation and CRM platforms to see if they offer tools.
 - Just because they say they are complaint, does not mean by default you are too



Creating an Action Plan

A child in a superhero costume, including a mask and a cape, is shown from the chest up. The child's arms are raised in a celebratory gesture, with one hand near their head and the other pointing upwards. The background is a plain, light color.

Not a Freak-Out Plan

Enforcement begins *May 25, 2018*

PX takes a team.



Creating a Plan



Data Collection Points

- What are we collecting & why
- Active vs. passive
- Storage & encryption
- Integration points



Messaging and Consent

- Opt-in language
- Privacy policy & legal documents
- Internal messaging around value and marketing impact



User Control

- Data portability
- Revoking consent
- Data erasure

Next Steps

- Legal should assess risk
- Create/update security and privacy policies
- Technology teams prioritize remediations
- Implement remediations
- Document remediations and next steps
- Rinse and repeat



A woman with long brown hair is carrying a young child on her back. They are in a grassy field with trees in the background. The sun is low on the horizon, creating a strong backlight effect and lens flare. The child is wearing a striped shirt and the woman is wearing a light blue top. The overall mood is warm and intimate.

PX is the new
Golden Rule

Drupal and Privacy/Security

[GDPR module](#)

[Guardr security distribution](#)

[Encrypt module](#)

[GDPR Consent module](#)

[Drush sql-sanitize](#)



[Privacy Concerns as GDPR Compliance \[#2848974\]](#)

[EU Cookie Compliance](#)

[GDPR Export module](#)

[Commerce GDPR](#)

What Did You Think?

Locate this session at the DrupalCon Nashville website:

<http://nashville2018.drupal.org/schedule>

Take the Survey!

<https://www.surveymonkey.com/r/DrupalConNashville>

Thank you!



Come See Us at Booth
#525

Join Us at our Afterparty
Tuesday 7-11pm @
The George Jones

Thank you!



@Mediacurrent



facebook.com/mediacurrent



Mediacurrent.com