ESPC
Email Sender & Provider Coalition

GDPR & ePR

Practical considerations for martech companies

Heather Goff, Oracle Marketing Cloud
Alex Krylov, Experian Cross-Channel Marketing

ORACLE

Today's Agenda

1. Overview of GDPR and ePR
2. Getting current with the times
3. Personal information
4. Challenges ahead
5. Journey to compliance
6. Checklist

These materials are prepared for educational purposes and are not intended as legal advice.

Evolution, not revolution in privacy regime

"This will impact every entity that holds or uses European personal data both inside and outside of Europe."

- Stewart Room

"This is not a transformation. …It is about making sure that the principles of the 1995 Directive are taken into account by businesses from the start."

- Vivienne Reding

Overview GDPR and ePR

And why ‘martech’ companies and their customers should care

What is the General Data Protection Regulation (GDPR)?

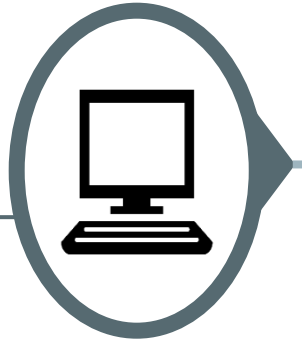
- The GDPR is a law in the European Union (EU) designed to enhance data protection for EU residents
- Replaces the 20 year old Directive (95/46/EC)
- Provides a framework to guide business usage of personal data across the EU
- All organizations processing PII (personally identifiable information) of EU residents must comply
- Significant penalties of up to 20 million EUR or up to 4% of annual worldwide turnover (revenue)
- Deadline for compliance is May 25, 2018

GDPR Timeline

January 10th 2017

GDPR is proposed + 4 years of political negotiations and lobbying

Final text of GDPR agreed upon by EU Parliament, Council and Commission



April 14th 2016

The EU parliament formally approved GDPR

May 25th 2018

GDPR becomes law and goes into force and becomes enforceable

What is the Regulation on Privacy and Electronic Communications (ePR)?

- The ePR is a proposed (draft) law designed to modernize "Cookie" Directive (Directive 2002/58/EC)
- Covers specific processing of all electronic communications, including new tech (E.g. IoT, VOIP, beacons) and types of data/metadata
- Applies stringent consent rules to cookie, non-cookie and cookie-like tracking
- Impacts direct marketing; addressable, online and mobile advertising; cross-channel and cross-device efforts
- Drafts attempt to harmonize with GDPR, including penalties
- ***Much is still unsettled and changes are being called for***

ePR Timeline

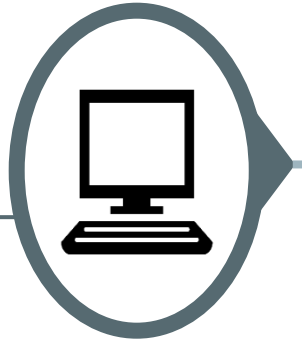
Dec 12th 2016

Initial draft text replacing ePrivacy Directive leaked

Draft text of ePR published by European Commission

April 4th 2017

Opinion issued by Working Party expressing concerns about 4 key areas



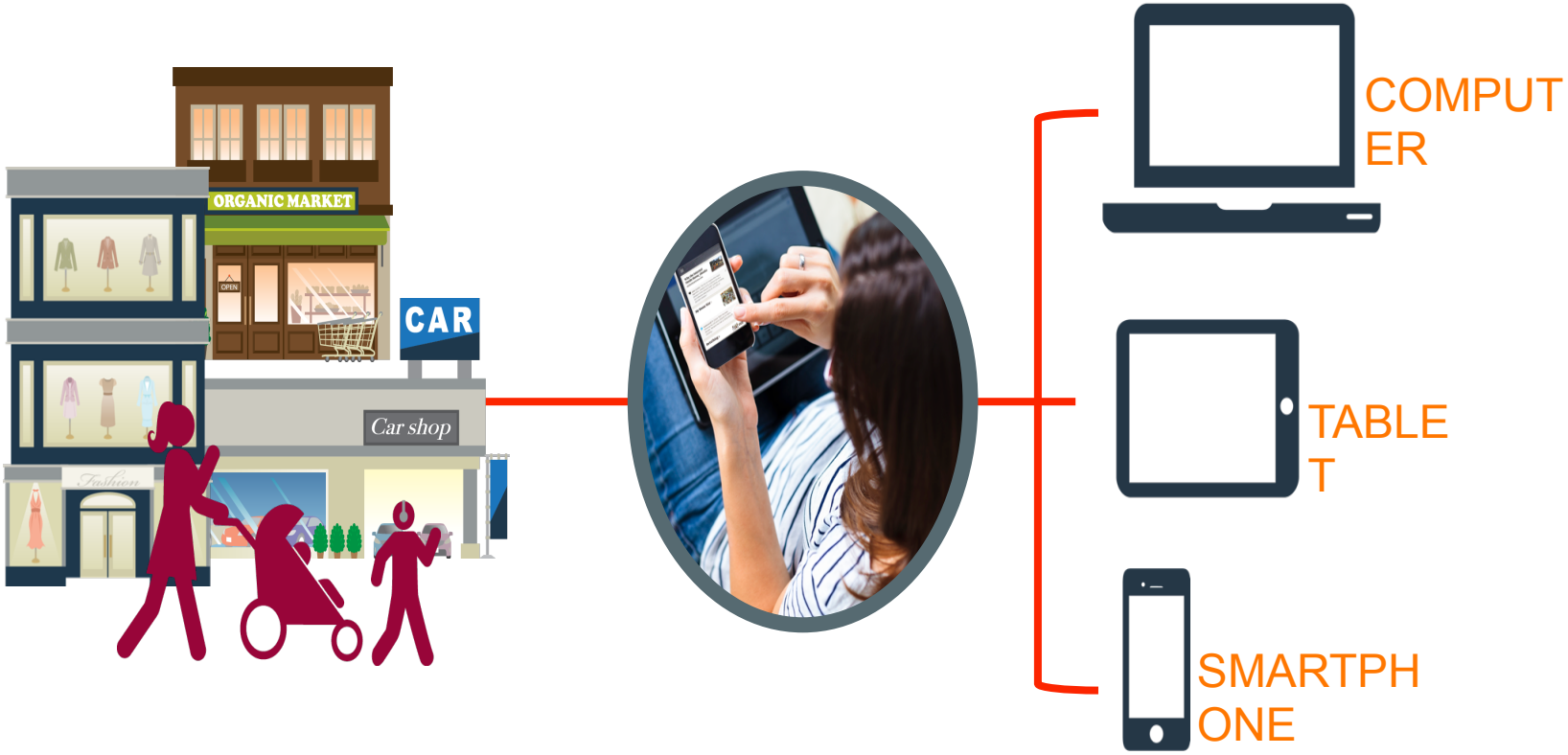
April 6th 2018

Blog posted by UK ICO highlighting impact on PECR and ICO's responsibilities

Getting current with the times

Technological developments = new data environments

New intrusive and potentially intrusive privacy contexts



Martech companies not in Kansas anymore

- **GDPR** regulates data processors
- Definition of PI broader than PII in the States
- Int'l data flows are just one piece of the GDPR puzzle
- Underlying systems and data governance processes need re-engineering to have privacy "by design"
- **ePR** may disrupt adtech industry (x-site, x-channel, x-device etc)
- Can't hide as intermediary behind contracts and thick privacy policies
- Need to demonstrate own compliance as tech enterprise

Wrestling with ‘Personal Information’

What's identifiable? GDPR makes context very important

- GDPR applies to the processing of all personal data
- GDPR expands on the type of data used in the **context of identifying individuals**

GDPR Article 4: *'…an identifiable natural person is one* ***who can be identified, directly or indirectly****, in particular* ***by reference to an identifier*** *such as a name, an identification number,* ***location data, an online identifier****, or to* ***one or more factors specific*** *to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.'*

ePR: Electronic Communications Data in scope

Mobile

- Device MAC
- Location data
- Wearables' data
- Mobile Device IDs
- App data
- Directory data

Online

- Email address
- Cookies
- Websites behaviors
- Email behaviors
- Tweets
- Likes
- Browsing history
- Communications
- IP address
- Purchases

Offline

- Name
- Home address
- Phone number
- DOB
- Facial recognition
- Civil registries
- Work, health, fin records

ePR: Tech and use cases in scope

Electronic Communication Services	Tracking	Marketing uses	Hazardous
VOIP	HTTP Cookies	Direct marketing	Cache / history sniffing
Instant Messaging	Tags / pixels	IBA/OBA	Super / Zombie cookies
Webmail	Cached objects	Retargeting	NPI to CRM
Social media	Browsing sessions	Social display	Clickjacking
Wearables	Headers	Onboarding	Location over time
Connected gadgets	Fingerprinting	Linkage/sync	
Wifi hotspots	Mobile IDs for Ads	Addressability	
	Search	Audience creation	
	Location beacons	Personalization	

Challenges Ahead

Everyone is chasing people-based marketing…
Email is #1 deterministic identifier in today's multi-channel reality…

Challenging areas to consider

1. Principles of personal data treatment
2. Lawful processing
3. Consent
4. Children
5. Individuals rights
6. Accountability and governance
7. Subject Access Requests
8. Breach notification
9. Transfer of data
10. International considerations

Onboarding challenge: Lawfulness of processing

- Clients need to Identify direct and other forms of marketing as their legal basis for sharing PI with you, and to collect appropriate consent
  - What does their privacy policy say?
  - How/Where do they collect PI?
  - Sensitive data for marketing? (E.g. health, children, credit worthiness)
  - How do they collect (and demonstrate) valid consent?
- Can you safely support the client?
  - How are *your* internal and external privacy policies
  - Are you vetting your clients?
  - Are you managing risks to *your* business (E.g. caps on liabilities)?

Service challenge: Consent for direct marketing, tracking, retargeting etc.

- **GDPR:** Freely given, specific, informed and unambiguous indication of individuals wishes; verifiable
- **ePR:** Aims to simplifies cookie consent rules, exempts non-intrusive use-cases
- Advertising and marketing cookies: **not simple at all!**
- Consent through **browser settings** problematic
  - Some advocates want strong privacy settings by default with enhanced notices
  - General settings about cookies may undermine *meaningful* informed consent under GDPR
  - Cookie-based settings will not work for mobile, fingerprinting etc

Vendor headache: Subject access requests

- 30 days to comply with request for access, correction, deletion
- Do you have policies/procedures for refusing requests?
- Do your data retention policies make sense?
- If B2B, do you have processes to rout requests to your data controller customer?
- Are you prepared to honor deletion requests?
- Meaningful opt-out may be more than “stop email” or “block cookie”:
  stop processing; stop linkage; stop re-association; null out ID, etc

Organizational challenge: Accountability and governance

- Financially, how do you think about the costs associated with data protection and privacy – do you expect a material change?
- Do you have any privacy compliance/data protection officer in place? Where?
- What kind of compliance framework, security, and training do you have in place in relation to data protection?
- How reliant is your business on the use of personal data?
- How central would you say use of data/data analytics is to your business model?
- How do you monitor what data you hold? What consumer data do you currently hold and in what
- Format (physical/electronic)? Do you know where the personal data you hold is stored (especially if it is in the cloud) and who has access to it?
- Do you have an accurate picture of what consents your customers have to use your services?
- How robust are your contracts with customers? Your own vendors?

The Journey To Compliance for 2018+

12 months to go to GDPR… 18 months for ePR?

Compliance Journey

2. Develop Plan

- About a year remaining to prepare before May 2018
- Detailed gap analysis

3. Build Consensus

- Make the case, show pros and cons
- Tell a compelling story with threats and opportunities

1. Assess Readiness

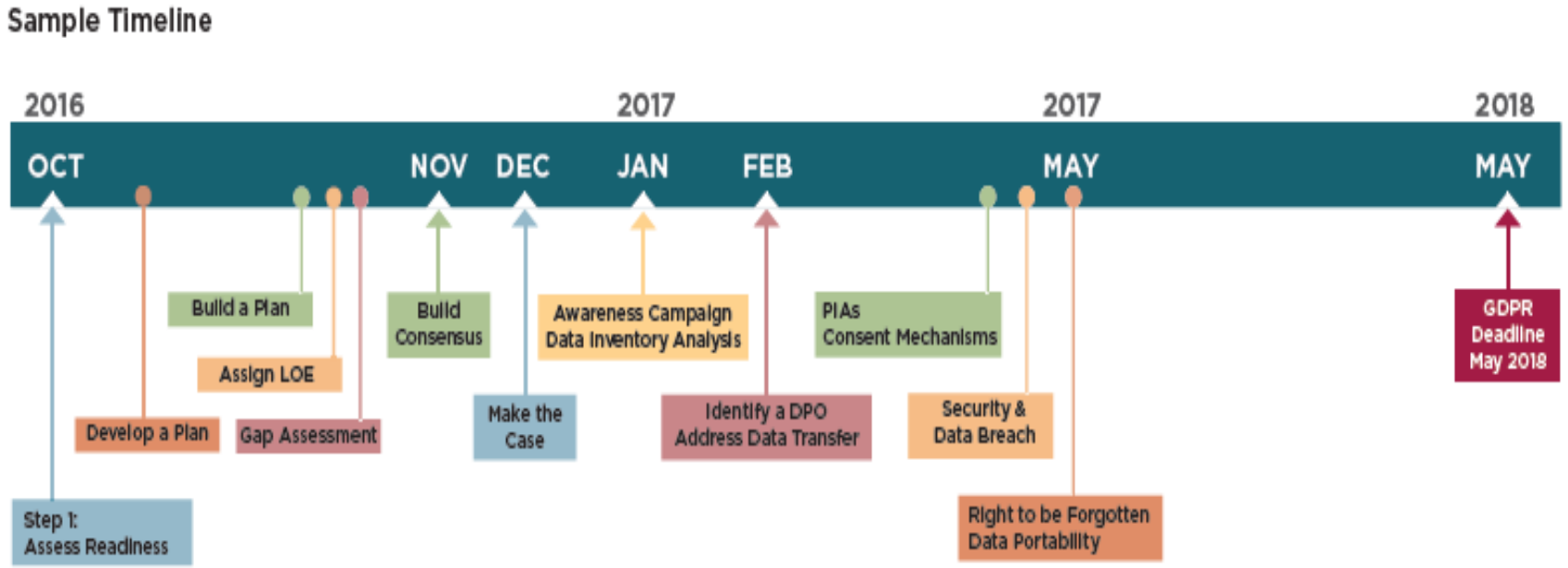
- Make leadership aware
- Gain appreciation of impact
- Get a comprehensive list of requirements
- Do you have a risk committee? A DPO?

4. Implement & Operationalize Viable Program

- Hiring new personnel
- Trainings and new processes
- New technology
- Data mapping and transfer, conduct DPIA

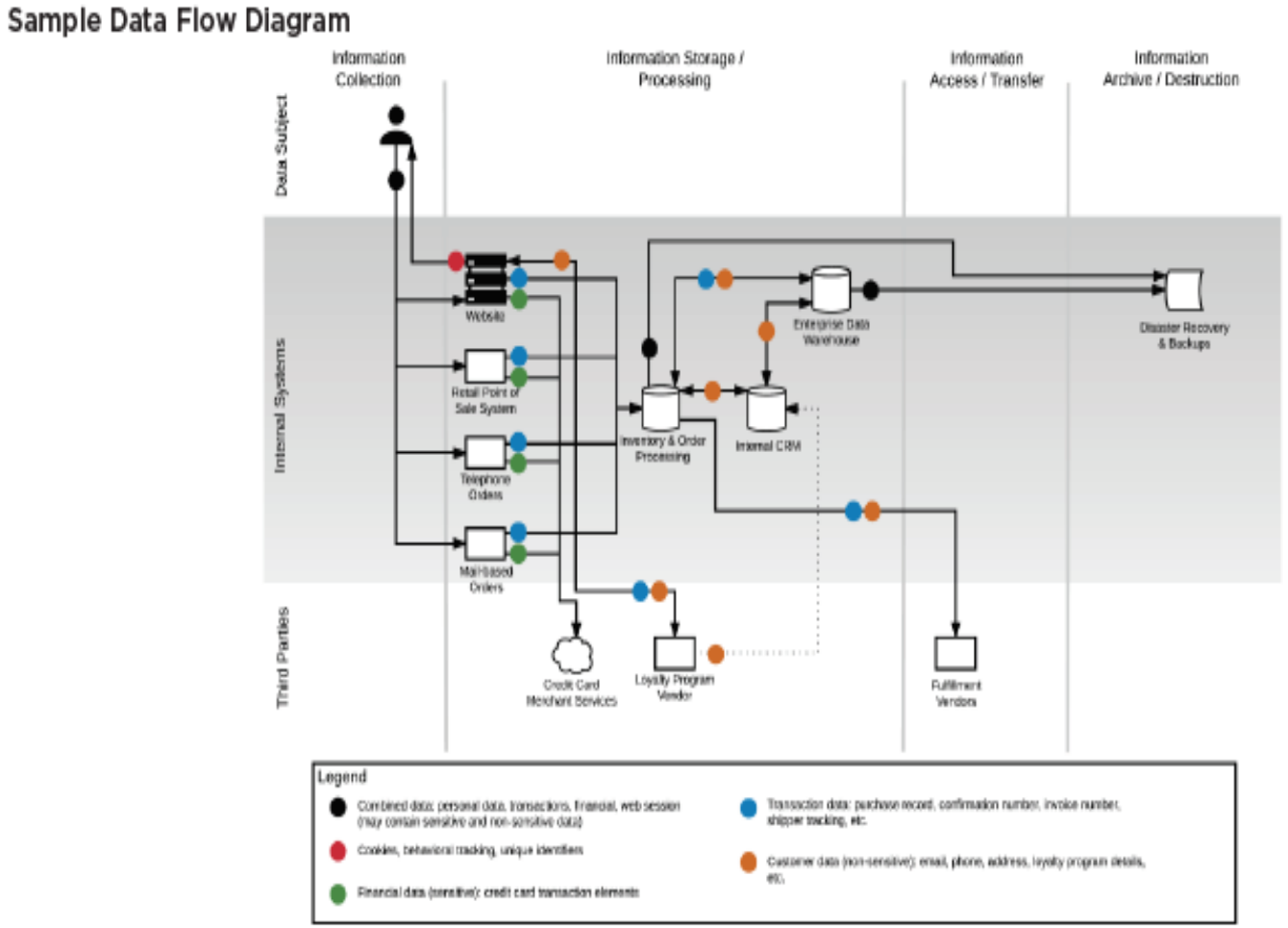
Do you have an implementation plan (and budget?)

Once you have gap analysis and risk assessment build out project plan



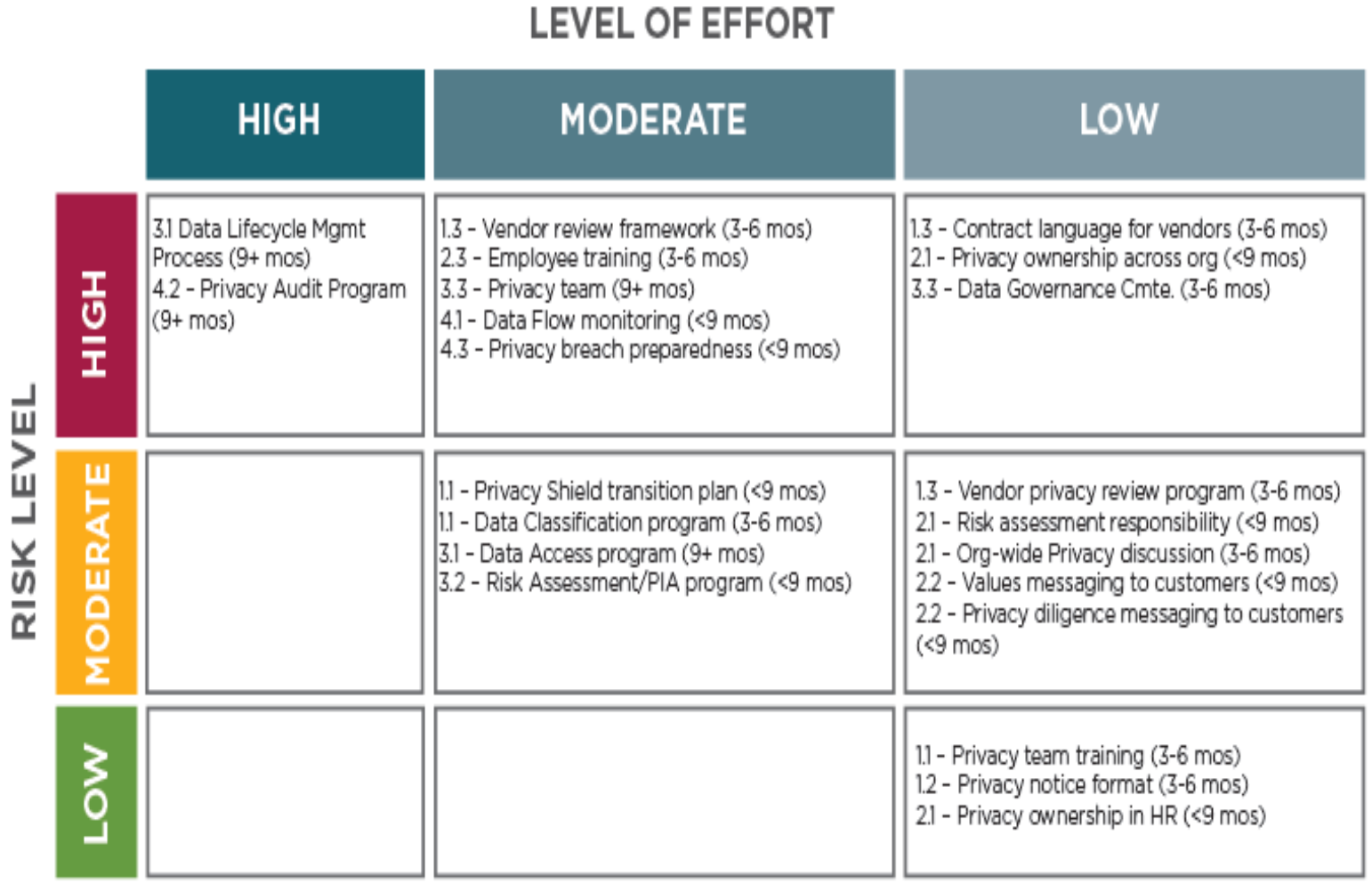
Source: TRUSTe EU GDPR Privacy Compliance G

Have you mapped and analyzed your data and flows?



Source: TRUSTe EU GDPR Privacy Compliance Guide: 2016

How serious and costly are your gaps?



Source: TRUSTe EU GDPR Privacy Compliance Guide: 2016

Use Case Example: Retargeting

A confluence of GDPR and ePR considerations

Shopping cart abandonment

Cross-channel solicitation automatically triggered by online behavior that is deterministically associated back to a natural person.

Preparedness checklist

GDPR

- ❑ Assign preparedness leader
- ❑ Map personal data processing
- ❑ Review legal basis & consents
- ❑ Prioritize actions
- ❑ Assess & mitigate risks
- ❑ Enhance internal processes
- ❑ Document *your* compliance

ePR

- ❑ Review your privacy policy
- ❑ Follow latest developments!
- ❑ Review consents for digital marketing
- ❑ Review opt-out capabilities
- ❑ Control for PI/PII leakage
- ❑ Control sensitive uses
- ❑ Extend commitments downstream
- ❑ Privacy-by-design for solutions

END. Questions?

- Heather Goff
  Strategic Services
  Oracle Marketing Cloud
  heather.p.goff@oracle.com
  Twitter: @HPGchatting
- Alex Krylov
  Privacy and Compliance
  Experian Cross-Channel Marketing
  alex.Krylov@experian.com
  Twitter: @akrylov

Thank you for your time.