# Everything You Need to Know About
# EU General Data Protection Regulation*

* But Were Afraid To Ask (Until Now)

#ILTAG89

# SPEAKERS

## Ian Raine

Director, Product Management

iManage

## Jeff Hemming

Product Manager, Marketing Solutions

Tikit Inc.

## Robert Cruz

Senior Director, Information Governance

Actiance, Inc.

## Grant Shirk

Vice President, Marketing

Vera Security, Inc.

# what is the gdpr, really?

# GDPR IN A NUTSHELL

- General Data Protection Regulation is a new EU law that consolidates the data privacy laws of all 28 EU Member States
- All of these member states already have privacy laws, but the GDPR consolidates them, and introduces some key new obligations on data processors and rights for individuals

Tough penalties
4% of annual revenue or
20 million euros

Regulations apply to non-EU companies that process personal data on EU citizens

Broader definition of personally identifying information

- Genetic
- Economic
- Mental
- Social identity
- Cultural

Controllers must report the breach within
72 hours

Data processors can be held directly liable for the security of personal data

You have to comply with GDPR by
May 2018

# IMPLICATIONS FOR US COMPANIES

- "Territorial reach" or "extraterritoriality"
  - Rules follow the data
  - US companies are impacted even if they are not located in EU but:
    - Offer goods or services to EU citizens, or
    - Monitor the behaviour of EU citizens
- EU definition of PII is broader than US

# HOW CAN EU FINE US COMPANIES?

- For US companies with a presence in EU, GDPR can be enforced directly on them by EU member state authorities
- If no presence, then GDPR requires companies to designate a representative located in the EU
- International law

where is all my data?

# KNOWING WHERE YOUR DATA RESIDES

Businesses must review and monitor their current processes, understand how PII (personally identifiable information) flows in and out of their business, what personal data they process, the grounds on which they are processing it and how it is secured.

= contains high % of structured PII

= contains mixture of unstructured doc types

what if my data isn’t clean?

# CLEAN DATA IS GOOD FOR BUSINESS

- GDPR enforces respect for contact information
- Rebuilds trust with clients and prospects
- For communications, is really applying best practices
  - Transparency
  - Easy access
  - Control

# EXISTING DATA - PRE-MAY 2018

Understand how to **IDENTIFY** Personally Identifiable Data (PII)

Create active processes to:

- Obtain **CONSENT!!!**
- Manage PII

Modify **TECHNOLOGY** to support compliance

**DOCUMENT** your data processes

- How data is identified and 'cleaned'
- Who is responsible
- Make it accessible and part of training

# NEW DATA– POST MAY 2018

Continue to get CONSENT and manage data

Create EASY tools for contacts to:

- provide consent or remove consent
- request information
- update PII
- transparently show the message origin

Monitor 'EXPIRY DATES' on consent

Review and enforce data RESPONSIBILITY procedures

is control really that important?

# CONTROLLING THE DATA

Let’s discuss specific use cases...

# WHO IS CONTROLLING YOUR DATA?

- GDPR applies to firms – and to data 'controllers and processors' that manage data for specific use cases
  - Cloud storage providers that retain data for regulatory compliance
  - Litigation service providers that manage data during eDiscovery
- GDPR provides opportunity to inspect existing data privacy and security protections built into those services
  - Technology + processes + skilled personnel

# KEY PROVISIONS OF GDPR


Right to be informed about how personal data is used


Right to request that personal data be deleted


Data controllers' obligations:

- Secure and manage personal data
- Regular 3rd party audits to ensure controls are enforced

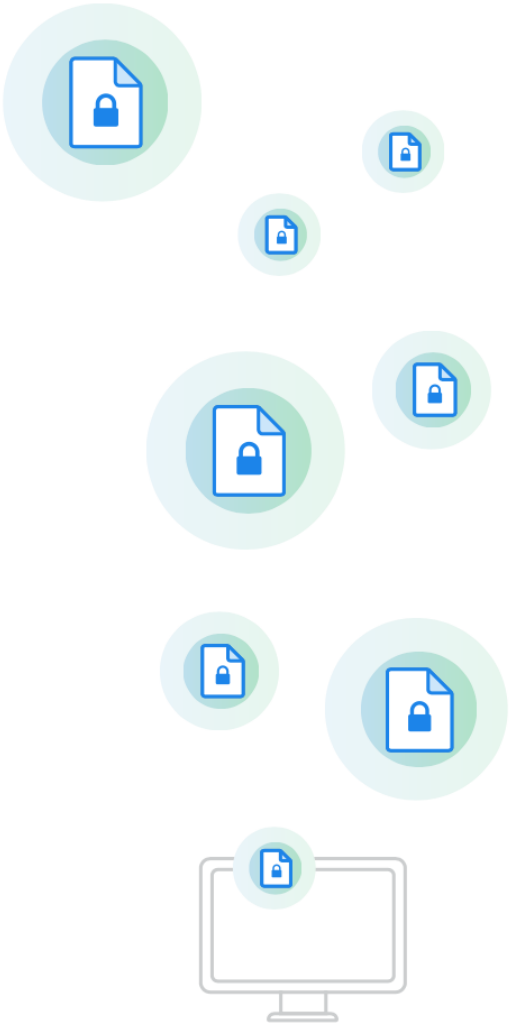
# QUESTIONS FOR YOUR SERVICE PROVIDERS

- Where is my data being stored?
- Does the service operate with Privacy by Design?
- Is access to my data limited only to authorized individuals?
- How fast can you respond to EU citizen inquiries?
- Can you honor the Right to be Forgotten?

can security and privacy be successful partners?

# MAKING SECURITY AND PRIVACY WORK TOGETHER

Over the last 18 months, **security, encryption, and access controls** have become regulators' top priority



## THESE REGULATIONS AREN'T COMPLETELY NEW, BUT THEY ARE DIFFERENT IN ONE MAJOR RESPECT...

The new rules are focused not just on protecting information systems but on securing, auditing and the disposition of data itself.

# Security, Access Control, and Breach Mitigation are Key:

## Traditional approaches to data loss can't address these 8 articles

### Strong Data Protections


**ARTICLE 5**
Personal data must be protected and used for only specific purposes


**ARTICLE 9**
"Special categories" of personal data must carry extra protection


**ARTICLES 25 & 32**
Data protection by design, and by default, ongoing protections and tracking

### Flexible Data Controls


**ARTICLE 17**
Right to be forgotten. On request, all personal data must be destroyed

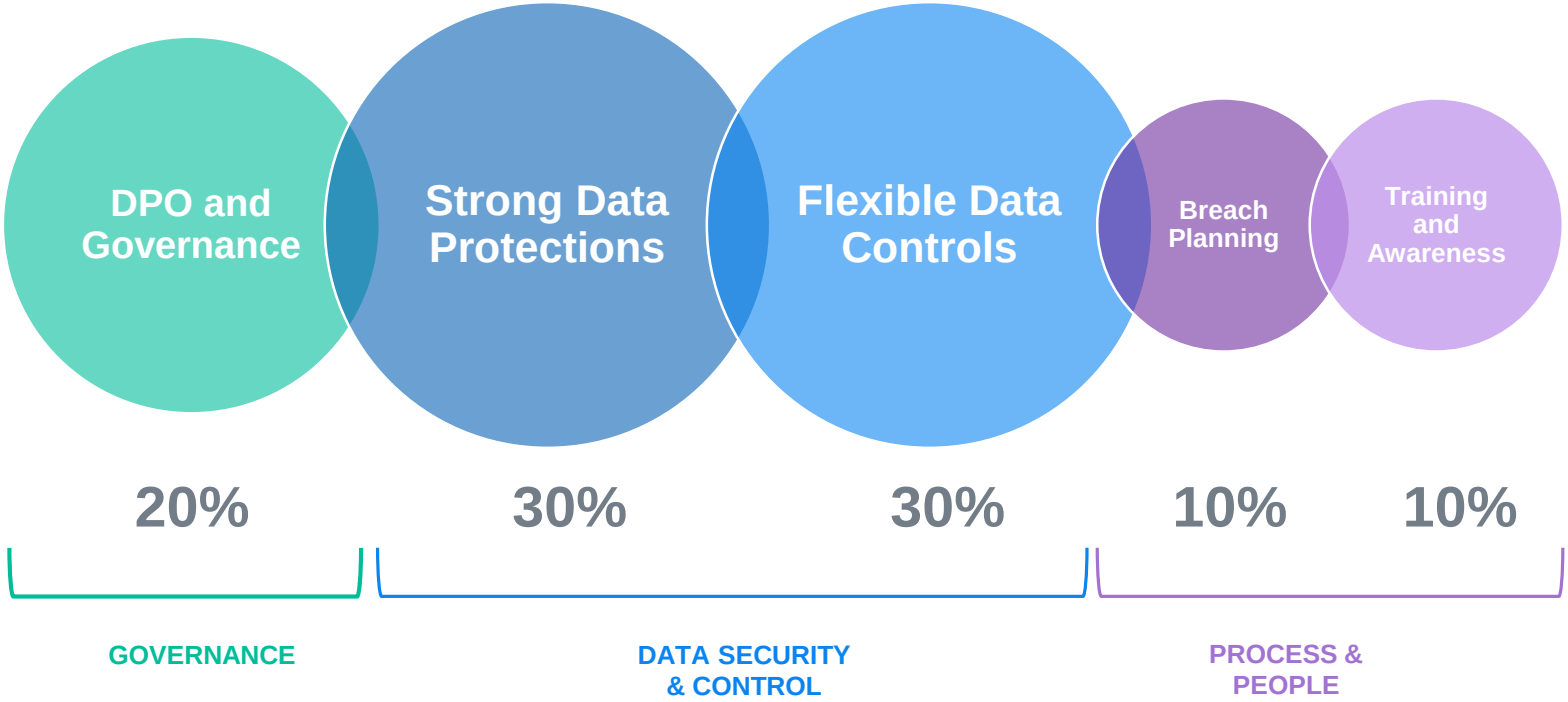

**ARTICLE 28**
Data controllers can only use sub-processors with adequate security

### Breach Impact Mitigation

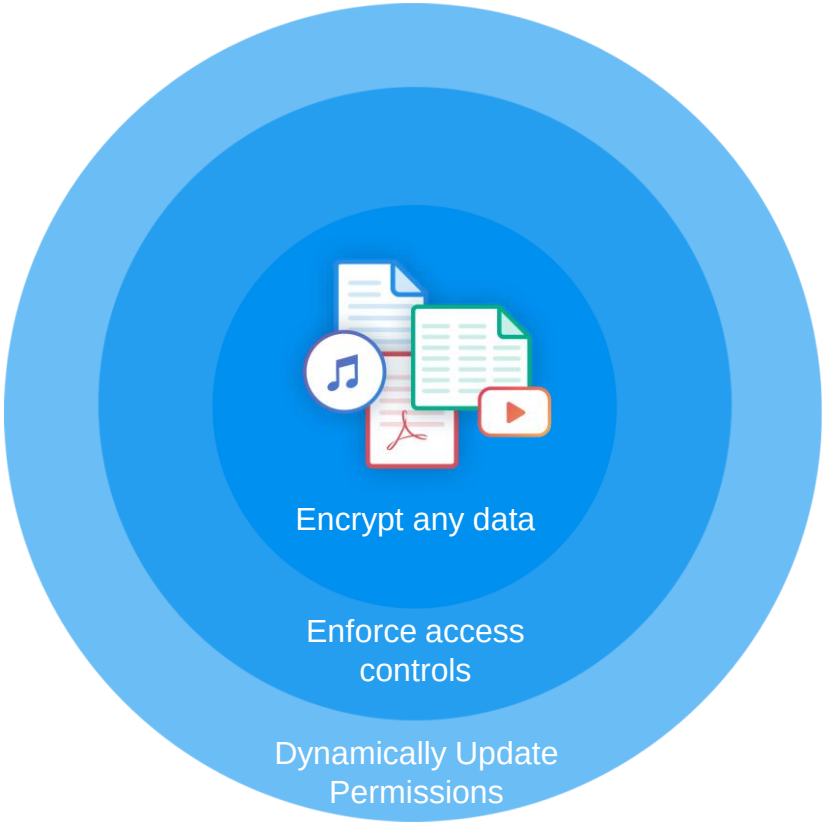

**ARTICLES 33 & 34**
72-hour breach notification. Any data not encrypted is not required to be disclosed


**ARTICLE 30**
Maintain records of processing activities, who had and has access to data

# Five steps to managing this risk



# A New Approach: Protect the Data Directly




Impenetrable as possible

Invisible to end users

# BREACH MITIGATION:

## THINK PREVENTION, NOT SUPPRESSION

# KEY TAKEAWAYS

- Catalog your data
- Consent!!!
- Ask: built for privacy by design?
- Protect what matters: the data

# QUESTIONS?