



# Data Privacy, Data Protection, and GDPR. What Does This Mean for Your Organisation?



14 September, 2017



**Information is your most important asset.  
Learn the skills to manage it.**



**The Community for  
Information Professionals**

[www.aiim.org](http://www.aiim.org)

# Thank You To Our Sponsors



# Today's Presenters



**Moderator:**

Theresa Resek, CIP  
Director  
AIIM



Thomas LaMonte  
Analyst  
AIIM



Ralph T. O'Brien  
Principal  
REINBO Consulting Ltd



Hazel Grant  
Partner  
Fieldfisher, London

# Today's Presenters



Ben Miller  
Business Development  
Konica Minolta



Bryant Bell  
Product Mktg Mgr –  
Archiving & GDPR  
OpenText



Julian Cook  
VP of UK Business  
M-Files



Andrea Chiappe  
Dir of Innovation & Strategy  
Systemware

# Today's Presenters



Reynold Leming  
Managing Director  
Informu Solutions Ltd



Marc Stephenson  
CTO  
Metataxis



Robert Perry  
VP, Product Management  
ASG



Paul Lanois  
VP & Senior Legal Counsel  
Credit Suisse

# Thomas LaMonte, Analyst

## AIIM





# GDPR

## We're All Going to be Fine(d)!

The Information used in this presentation is based on an AIIM survey conducted May, 2017



# Time Left till ~~DOOMSDAY~~ GDPR Comes into Force

|      |   |       |   |         |   |         |
|------|---|-------|---|---------|---|---------|
| 252  | : | 11    | : | 9       | : | 38      |
| Days |   | Hours |   | Minutes |   | Seconds |

...What Was Life Like Before GDPR?



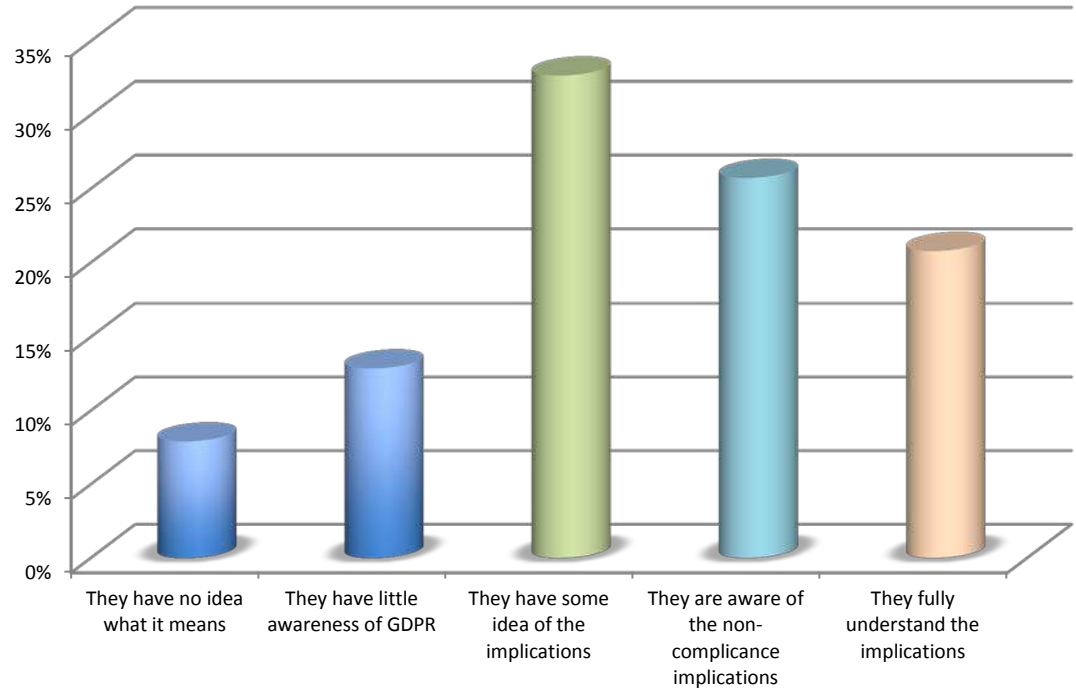
# Not So Fast... What does GDPR Stand for?



- a) Grains, Dairy, Produce, and Ramen
- b) Graduate Degree Progress Report
- c) Gross Domestic Product by Region
- d) Grateful Dead Public Radio
- e) General Data Protection Regulation

# How would you rate the level of understanding your executives have of the implications of GDPR non-compliance?

- 21% feel their executives fully understand the implications of GDPR
- 8% say their executives have no idea of GDPR implications





# What's the Big Deal? Sanctions



- A warning in writing in cases of first and non-intentional non-compliance.
- Regular periodic data protection audits.
- A fine up to **10,000,000 EUR** or up to **2% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4).
- A fine up to **20,000,000 EUR** or up to **4% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 5 & 6).

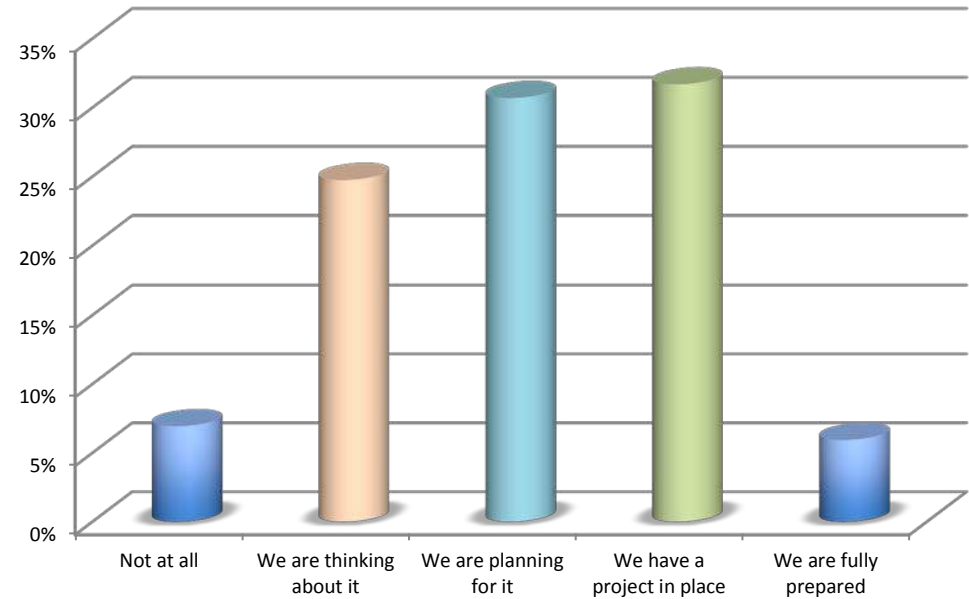
No Sweat...Everybody's Ready Right?



Yeah, We Got This

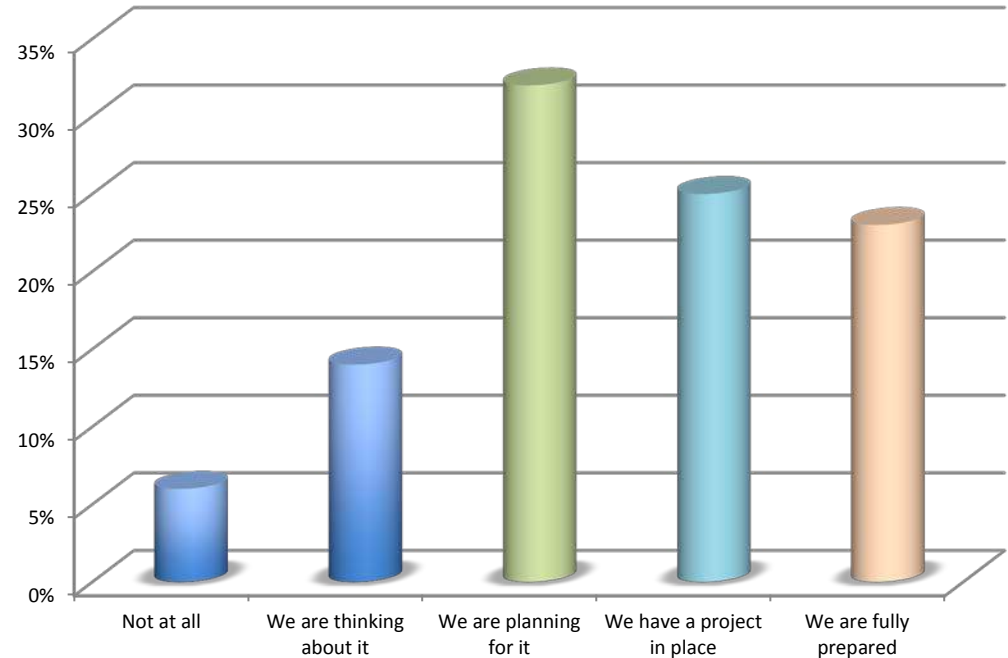
# How would you rate the readiness of your organization in meeting the GDPR requirements now?

- 6% say they are fully prepared
- 7% have not even begun to prepare




# How would you rate the readiness of your organization in meeting the GDPR requirements when it is enforced in May of 2018?

- 6% say they will not even be close
- 23% feel they will be fully prepared





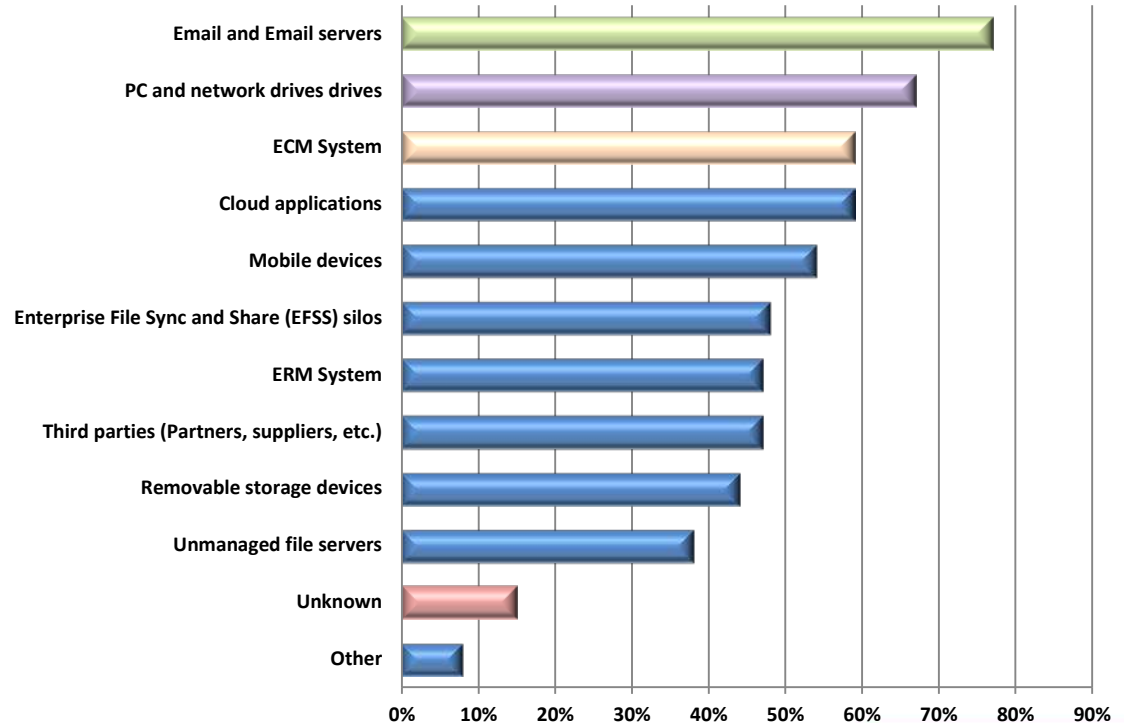
# Keeping Tabs On Our Digital DNA



Personally Identifiable  
Information (PII) can be  
extremely sensitive, but  
propagates everywhere

Understanding that there is PII data already managed within databases and Line-of-Business applications like Salesforce, etc., where do you feel GDPR impacted content is being sorted within the following:

- 77% cite email and email servers
- 67% cite PCs and network drives
- 59% equally cite ECM systems and cloud applications

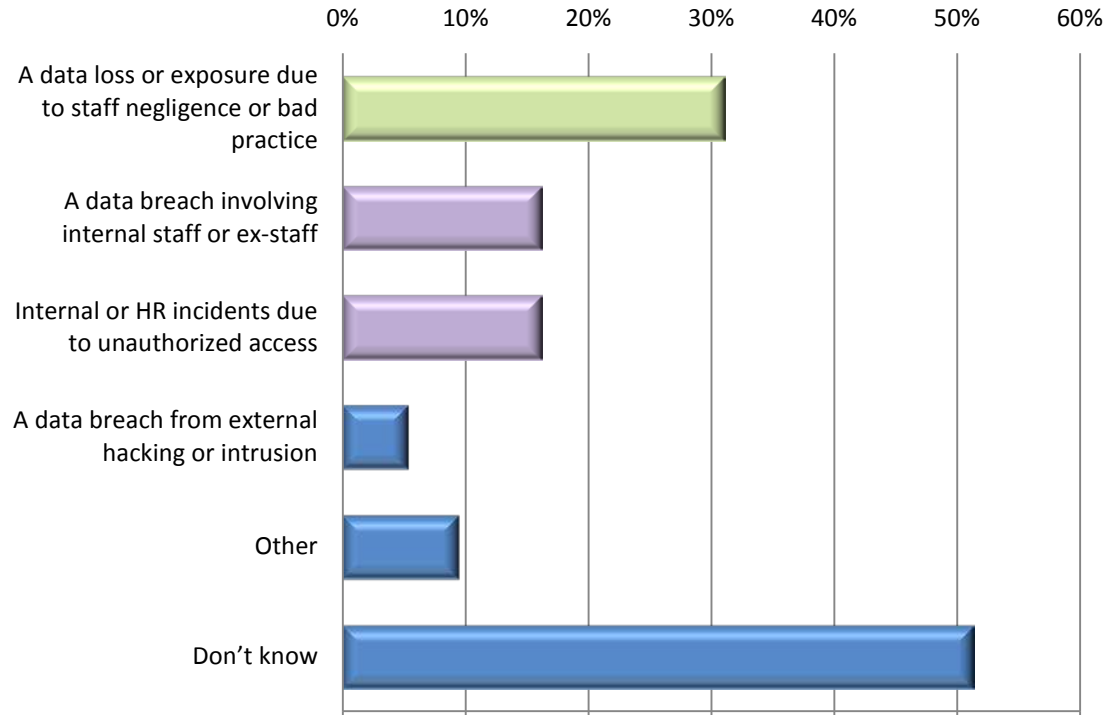


# The Security Risks You Don't Account For Hurt the Most



# Has your organization suffered any of the following in the last 12 months?

- 31% cite loss or exposure due to staff negligence or bad practice



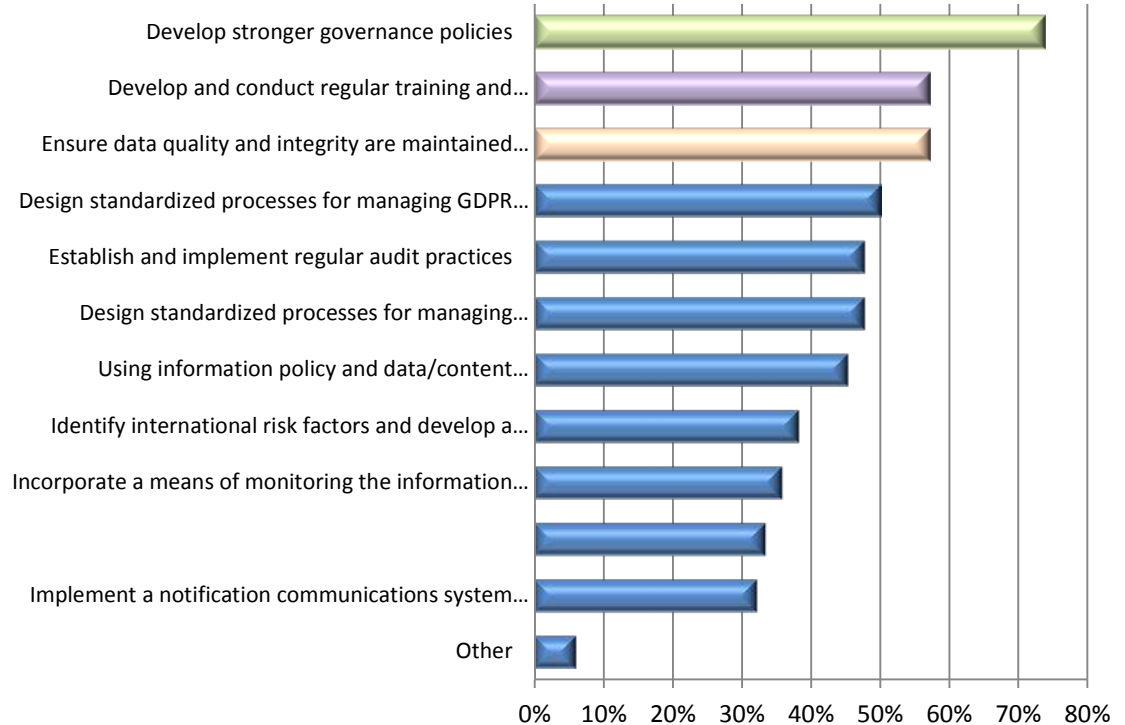


# Prepare Methodically, But Please Pick Up The Pace



# What actions will you be taking to prepare for May 2018 and compliance with GDPR?

- 74% will develop stronger IG policies
- 57% will conduct training and data cleansing exercises equally



# The Next Step Isn't Always Clear—Seek Out Help



## Best Practices:

- Know what you have for PII
- Create a “Helicopter” view
- Maximize metadata use
- Apply encryption technologies
- Control and monitor

## Remember:

- GDPR is global; everyone is affected
- If you’re not sure where to turn, seek out trusted advisors in the supplier community or professional associations
- Pursue quick wins and realistic goals. GDPR compliance is a process

# HOW TO REACH ME

- Thomas LaMonte, Analyst
  - [tlamonte@aiim.org](mailto:tlamonte@aiim.org)
  - [@TomLaMonte](https://twitter.com/TomLaMonte)
  - [www.linkedin.com/in/tlamonte](https://www.linkedin.com/in/tlamonte)
- Bob Larrivee, VP/Chief Analyst
  - [blarrivee@aiim.org](mailto:blarrivee@aiim.org)
  - [@BobLarrivee](https://twitter.com/BobLarrivee)
  - [www.linkedin.com/in/boblarrivee](https://www.linkedin.com/in/boblarrivee)

# Ralph T. O'Brien, Principal REINBO Consulting Ltd





# GDPR – A Strategic Approach & some HEADLINES busted

## HEADLINE #1

“I’m a GDPR Expert”

# Ralph T O'Brien

FIP CIPP/E CIPM MBCS CiISM

Ralph has spent nearly two decades working at the intersection of privacy, security and risk management.

Assisted global organisations to improve their privacy governance as part of sustainable management systems across global enterprises

Completed customer projects such as Data Inventory, Data Mapping, GDPR Strategic Priorities Assessments, detailed GDPR assessments, and advisories around specific products and services privacy implications

Experienced speaker including at IAPP, IRMS, BCS, Data Protection Forum, NADPO and other conferences

Developed bespoke training materials for privacy and security, and worked with several vendors to develop tools and products in the privacy industry and introduce them to market

Utilises and creates governance frameworks including work on the ACPO Data Protection Audit Manual, British and international standards such as work on the BSI committees to create BS 10012 (the standard for Personal Information Management Systems)



Principal, REINBO Consulting Ltd

Previous: TrustArc, KPMG, BSI, Control Risks, Ultima Risk Management, IT Governance

# GDPR Experts?

No Accredited “GDPR” qualifications exists as yet.

Certification bodies (UK) are UKAS and the ICO only. Neither have approved any accredited qualifications.

Many organizations are provide privacy/GDPR training courses – these provide limited assurance.

One week does not make a privacy pro!

Look for practical experience, track record of delivery and references.

Legal Advice and Consultancy are different skills, and provide different things!

All we have is the GDPR text, Recitals, and Regulator guidance.

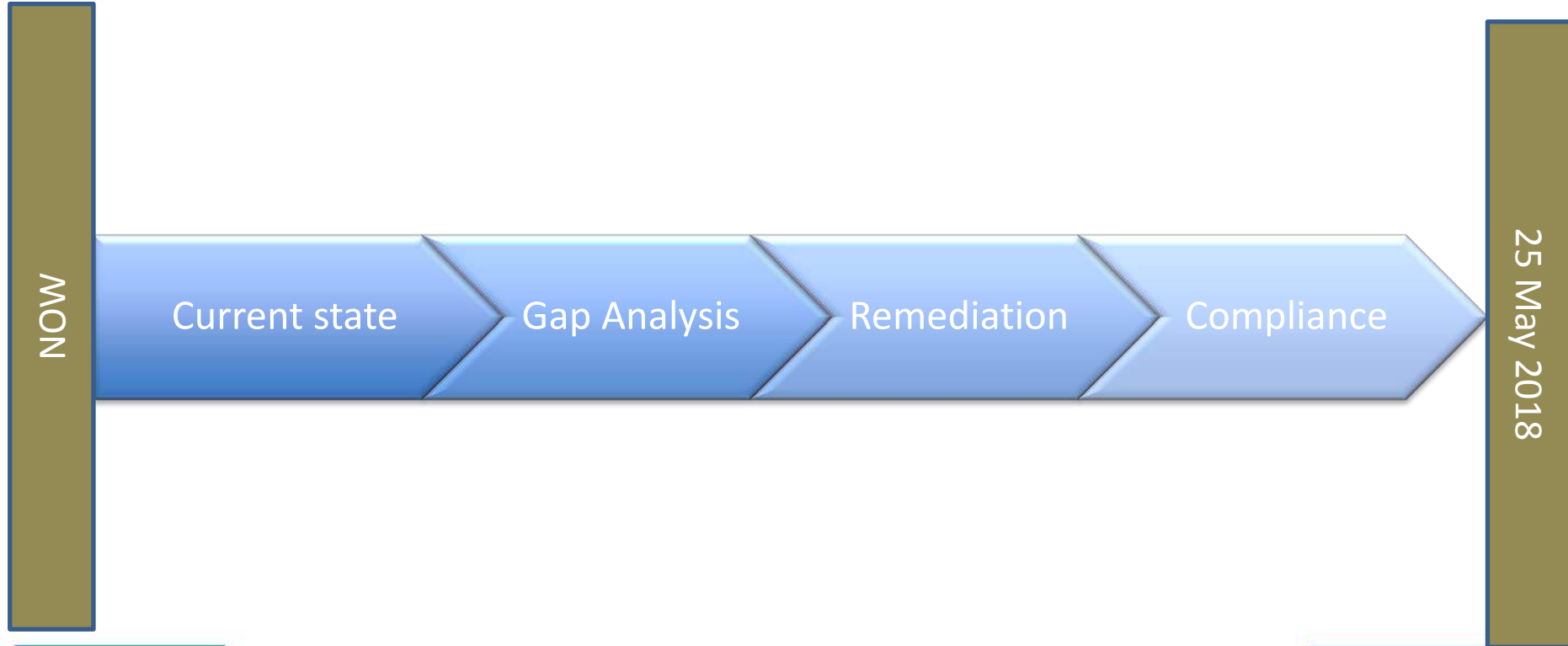
All compliance programmes are untried and untested.



## HEADLINE #2

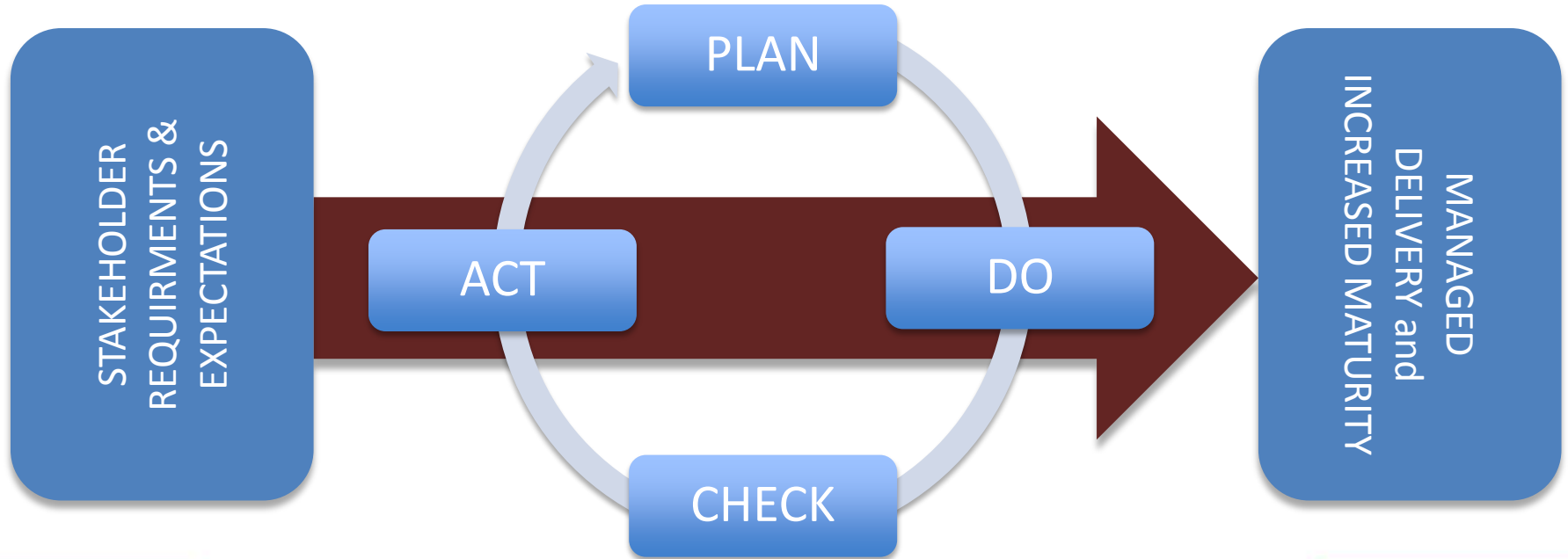
“I must be compliant by May 2018”

# Most Look at the Timeline Like This





# Privacy Is Not “One and Done”



# GDPR Enforcement – May 2018

What is compliance? Is there a binary YES/NO answer?

**Controllers and Processors must comply to the law.**

However, the law uses words like “adequate, relevant, necessary, appropriate” etc.

This means the focus is on the organization to prove it has “done its homework”

It is a risk management activity:

Valid options are to take, treat, tolerate, terminate or transfer the risk

Your response will vary based on who you are

Focus on High risk personal data processing areas first!

You may not want the “Gold Standard” in all areas



# Proactive Demonstration of Compliance

## [GDPR Article 22 \(extract\)](#)

The controller shall adopt policies and implement appropriate measures to ensure, and be able to demonstrate, that the processing of personal data is performed in compliance with this Regulation.

**New Requirement to “Proactively demonstrate” – Keep Records of Evidence**

## HEADLINE #3

“I will be fined 4% of global turnover or  
20,000,000 euros”

# Regulators

Regulators have different compliance options:

- Will normally work with you during investigation

- Can serve enforcement notices, stop notices, reach informal agreements,

- The maximum fine is unlikely as it represents “the worst privacy thing you can do ever”

Regulators will not arrive in May 2018 (or ever!) unless;

- You are a known target

- You have had a data breach

- You hit the headlines

- They receive complaints

Layer of Defense

- 1 – Not getting on regulators Radar (see above!)

- 2 – Having good records of compliance activities when they so

- 3 – Having plans to improve and mature going forwards

- 4 – The regulator could be a “critical friend”

## HEADLINE #4

“I Need to get ...  
Explicit consent,  
A data protection officer,  
Do data mapping,  
Right to be forgotten,  
etc., etc...”



# Get Out of the Specifics, Into the Programme...

## Strategic

- Set up a Continually Improving Privacy Programme
- Risk Based maturity model

## Tactical

- Ensure each business process complies with privacy principles
- Risk Based Prioritization

# Review Each Element for Your Maturity

| TOPIC                          | Desired | Current |
|--------------------------------|---------|---------|
| <b>Operating Model</b>         |         |         |
| Governance Model               |         |         |
| Privacy Office Management      |         |         |
| Privacy Office Planning        |         |         |
| Privacy Risk Management        |         |         |
| <b>Policies and Procedures</b> |         |         |
| Internal Privacy Policies      |         |         |
| External Privacy Policies      |         |         |
| Document Control               |         |         |
| <b>Security for Privacy</b>    |         |         |
| Information security           |         |         |
| Breach management              |         |         |
| Investigation/E discovery      |         |         |

| TOPIC                                       | Desired | Current |
|---|---------|---------|
| <b>Third Party Management</b>               |         |         |
| Supplier Due Diligence                      |         |         |
| Contracts Clauses                           |         |         |
| Assurance and Audit                         |         |         |
| <b>Stakeholder Management</b>               |         |         |
| Roles, Training and Competency              |         |         |
| Awareness                                   |         |         |
| Public Relations                            |         |         |
| <b>Monitoring and Improvement</b>           |         |         |
| Privacy control Monitors                    |         |         |
| Security Control Monitors                   |         |         |
| Independent Assurance and Corrective Action |         |         |

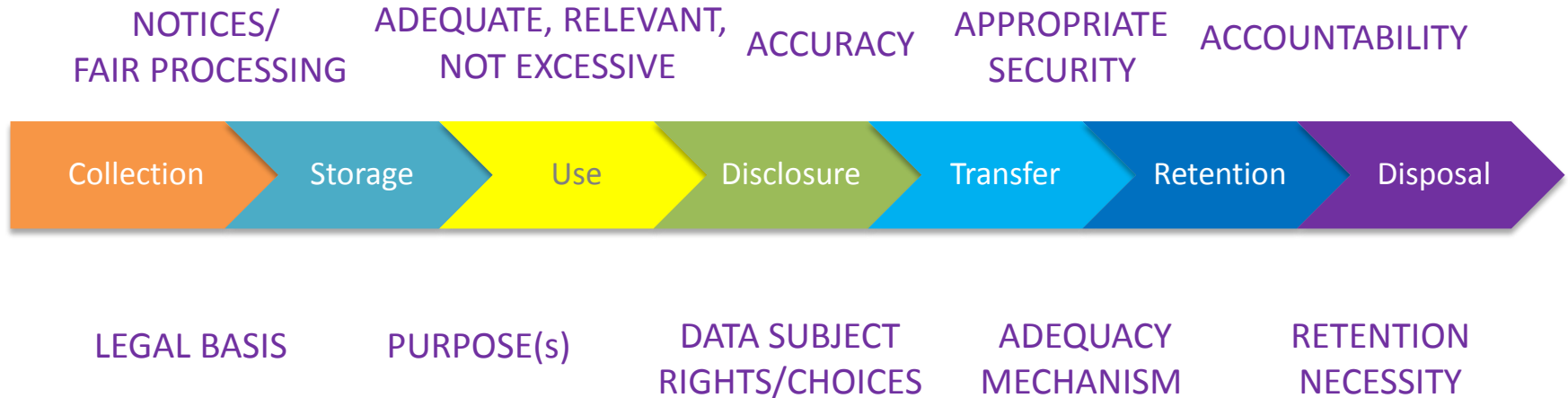
# Review Each Element for Your Maturity

| TOPIC                              | Desired | Current |
|------------------------------------|---------|---------|
| <b>Information Management</b>      |         |         |
| Anonymization processes            |         |         |
| Legal Basis/Purpose identification |         |         |
| Minimization processes             |         |         |
| Validation and Accuracy            |         |         |
| Notices and obtaining consent      |         |         |
| Withdrawing consent                |         |         |
| Children's data                    |         |         |
| Classification processes           |         |         |
| Retention processes                |         |         |
| Disposal processes                 |         |         |

| TOPIC                                     | Desired | Current |
|---|---------|---------|
| <b>Key Privacy Processes</b>              |         |         |
| Data Inventory and Mapping                |         |         |
| PIA and PbD                               |         |         |
| Regulator Interactions                    |         |         |
| Regulator Filings and registrations       |         |         |
| International Transfer mechanisms         |         |         |
| <b>Rights Management</b>                  |         |         |
| Complaints Process                        |         |         |
| Subject access Requests                   |         |         |
| 3 <sup>rd</sup> party disclosure requests |         |         |
| Rectification requests                    |         |         |
| Portability requests                      |         |         |
| Erasure Requests                          |         |         |

# Tactical – Business Processes vs Principles

Processes for Data Inventory, Risk management, Privacy Impact Assessment, Privacy by Design, Rights will drive compliance



# HOW TO REACH ME

Please Enjoy GDPR Responsibly

- Ralph T O'Brien
- FIP CIPP/E CIPM MCBS CiISMP
- Principal, REINBO Consulting
- Tel: +44 (0) 7920 107 959
- [robrien@reinboconsulting.com](mailto:robrien@reinboconsulting.com)

# Hazel Grant, Partner Fieldfisher, London





# GDPR – 5 Hot Questions

Hazel Grant, Partner  
Fieldfisher, London

# Q1: What's the real date?

- May 25, 2018
- The transitional/implementation period is now
- EU regulators expect to enforce starting immediately after May 25
  - Likely first actions against breaches?

## Q2: What about Brexit?

- GDPR in full effect 10 months before Brexit
- UK Government has said it will “implement” GDPR
- UK (and other Member States) will have local laws to “fill in the gaps/top up” GDPR
  - E.g., Data protection officer (DPO)

# Q3: What's the big deal?

- GDPR:
  - puts all the “best practice” guidance into law
  - means that vendors/service providers are now directly liable under data protection law
  - applies to businesses outside the EU, if they are targeting or monitoring EU residents

## Q4: What if I just ignore it?

- Possible fines of up to 4% global annual turnover or 20million euro, whichever is the higher
- Possible claims from individuals affected
- Possible orders from data protection authorities
  - E.g., to stop processing or stop international data transfers

## Q5: OK, so what do I do first?

- Know your data and data flows – carry out data mapping
- Review your policies, consent wording and contracts – they all need to be updated
- Document everything – you are now “accountable” for data protection compliance, so must prove your compliance

## HOW TO REACH ME

- Hazel Grant
- Partner, Fieldfisher, London
- [Hazel.grant@fieldfisher.com](mailto:Hazel.grant@fieldfisher.com)
- +44 207 861 4217
- +44 777 572 8838

# Ben Miller, Business Development Konica Minolta





# Konica Minolta | UK

Debunking the top 3 GDPR myths

# GDPR – the whole story

GDPR does cover 'data security'

But, GDPR also requires -

- Data breach management and reporting
- Data destruction
- Data migration
- Explicit consent
- The right to be forgot
- Processes and best practice
- Appointment of a Data Protection Officer

# 3 Myths about GDPR

1. ~~GDPR is just about stopping data breaches~~

# Single point solutions

GDPR is multi-faceted – no one piece of software will ensure compliance

Achieving GDPR compliance can be complex -

- Identification where PII data rests
- Securing existing content
- Access management around content
- Consent management and tracking
- Ongoing analysis of compliance
- Culture of good governance from the top down

# 3 Myths about GDPR

1. ~~GDPR is just about stopping data breaches~~
2. ~~GDPR compliance can be achieved with a single piece of software~~

# There isn't a finish line

GDPR compliance is not a project that has an end date

Even for those who are fully GDPR compliant in May 2018 the journey is just beginning -

- Ongoing checks
- Continued evaluation
- Reporting and monitoring

# 3 Myths about GDPR

1. ~~GDPR is just about stopping data breaches~~
2. ~~GDPR compliance can be achieved with a single piece of software~~
3. ~~GDPR is a project with an end date~~

# But it needs to begin

Every business will adopt it's own philosophy in achieving GDPR compliance -

- Take a consultative approach
- Identify the data you have
- identify potential areas of non-compliance
- Prioritise those areas based on potential impact



# HOW TO REACH ME

Ben Miller

Konica Minolta



[bmiller@processflows.co.uk](mailto:bmiller@processflows.co.uk)



<https://www.linkedin.com/in/ben-luke-miller>

# Bryant Bell, Product Marketing Manager – Archiving & GDPR OpenText

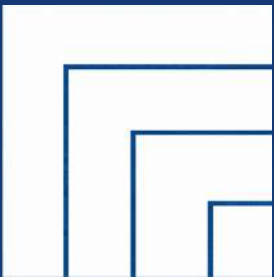


# Privacy by Design & Default

The Case for a Central Information  
Repository

# Agenda

- GDPR – The New Data Owner
- Personal Data – A Broader Perspective
- Privacy by Design & Default
- Compliance Option – Centralized Repository



# New Data Owner

- The Digital Economy
  - Data is a business asset
  - Personal data is leveraged everywhere
- GDPR makes it clear that:
  - Personal data is the property of the data subject
  - The data subject has new rights of visibility, erasure and portability

# Personal Data & Content



# Personal Data & Content



# People – Process – Technology

## People

- Changing Behaviors
- Consent

## Process

- Means to address inquiries
- Data lifecycle management

## Technology

- Find GDPR data
- Classify
- Control
- Ensure compliance



# People – Process – Technology

## Technology

- Find GDPR data
- Classify
- Control
- Ensure compliance

# People – Process – Technology

## Technology

- Find GDPR data
- Classify
- Control
- Ensure compliance

## EU Citizen's Rights

- Access
- Portability
- Erasure “Right to be Forgotten”

# Privacy by Design & Default

- Consolidated Repository – A Strategic Component
  - Secure access and control
  - Consistent retention and disposition
  - Quickly respond to Data Subject's requests
  - Streamline Audit and reporting
  - Future proof data
  - Compliant data source for analytics
  - Elimination of costly legacy systems



# Act Now

- Don't Delay
- Get Educated
- Seize the Opportunity

# HOW TO REACH ME

Bryant Bell

OpenText – Product Marketing



[bellb@opentext.com](mailto:bellb@opentext.com)



[@bell2bry](https://twitter.com/bell2bry)



<https://www.linkedin.com/in/bryantbell/>

More GDPR Info: <http://www.opentext.com/what-we-do/business-needs/information-governance/ensure-compliance/gdpr-are-you-ready>

# Julian Cook, VP of UK Business M-Files



# A Process-Based Approach to GDPR

Lowering the Risk  
While Keeping it Simple

# 31%

of organisations experienced  
data loss caused by staff negligence  
or bad practices

AIIM & M-Files, GDPR Readiness Research 2017



This is a process problem  
Not a technology problem





TIME IS RUNNING OUT

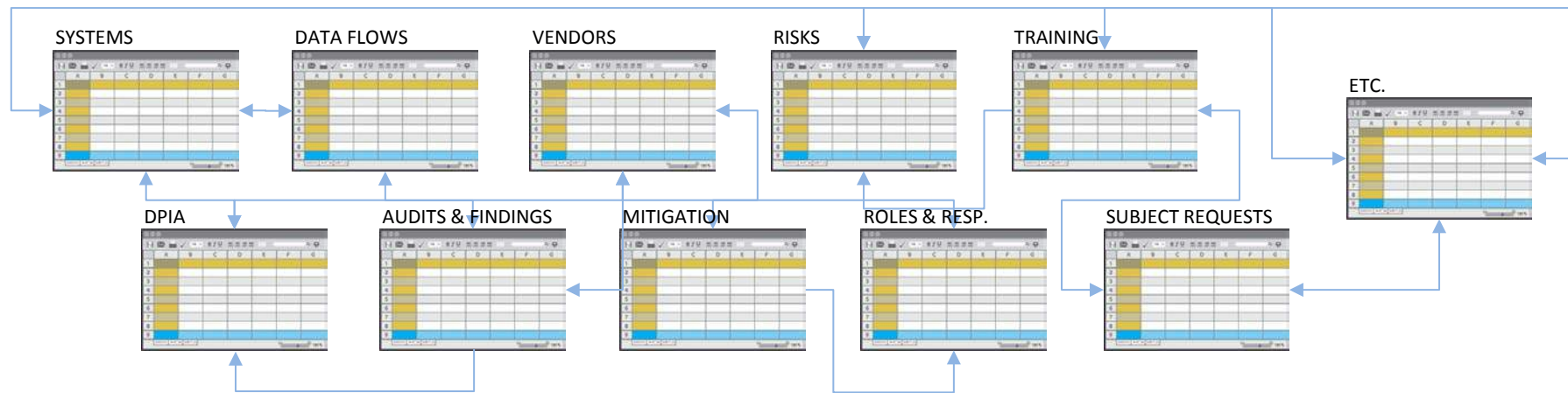
**DON'T PANIC**  
**START NOW**  
**GET HELP**

# Getting started: Is it difficult?

- Is GDPR compliance really that different?
  - Apply lessons learned from other compliance projects
- Is it simply the breadth of the issue?
  - Rank your risk exposure by business unit, system, vendor, etc.
- How to simplify?
  - Reduce the scale of the problem; Prioritise and address incrementally



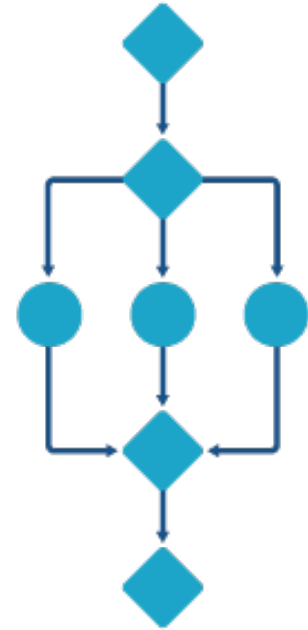
# Is Excel the answer?



- Unmanageable relationships and interdependencies
- Multiple versions of documents in different locations
- Information silos with no workflow or process automation
- Impossible to audit and prove – so what's the point?

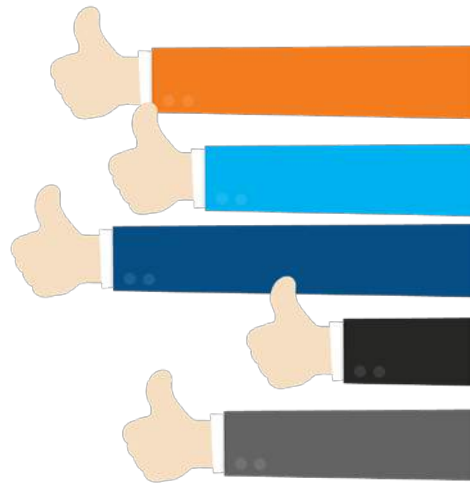
# Follow a simple, process-based approach

- Understand what you have and where it resides using a **personal data registry**
- Link **processes, documents, events, and activities** to the registry
- Define and communicate **policies and procedures** through automated training
- Ensure all **actions are recorded** for audit and reporting purposes



# How can this approach benefit you?

- Starting with a Personal Data or Information Asset Registry
  - Enables incremental roll-out of GDPR, based on vulnerability and risk
- Streamlining and automating GDPR related processes
  - Minimizes staff time and effort on compliance
  - Reduces risk of human error
- Built-in activity monitoring and recording
  - Proves to auditors that you are following best practices
  - Alerts you of potential GDPR non-compliance



# Key takeaways

- A simple, process-based approach to information governance provides a practical foundation for GDPR compliance
- No need to strive for perfect compliance right away. Focus on the foundation and best practices first
- Building in auditability from the ground up dramatically reduces the risk of GDPR non-compliance

# HOW TO REACH ME



Julian Cook

Vice President of UK Business, M-Files

[julian.cook@m-files.com](mailto:julian.cook@m-files.com)

**M-Files®**

# Andrea Chiappe, Director of Innovation & Strategy Systemware







# GDPR A FORCE FOR TRANSFORMATION

9.14.2017

Andrea Chiappe  
Systemware, Inc.



MAY 25, 2018



- Connect Silos
- Ranking Regulations
- User Processes
- Beyond Porting

# Fortune 25 Financial Company

## CHALLENGE



Petabytes of data



Months/weeks researching audit requests



Wasted time in cumbersome systems



Subject to several lawsuits and investigations



**Strict business continuity requirements**



**Disparate information systems and outdated legacy environments**



**60 million customers**



**Global regulations & compliance constantly evolving**

## SOLUTION



Content Cloud to manage governance and connect or migrate disparate systems



Provide context-centric & curated access to critical business information across the enterprise



Provide seamless interoperability between existing systems



Capture convert, curate, and distribute billions of documents, reports, meta data and images



100% availability



Provide content analytics



Content accessible immediately at any location around the world

## RESULT



Billion report pages captured



Billion statement pages captured



Million account records



**Customer service markedly improved**



Reduction in paper statements



**Meets stacked regulatory, compliance, record, retention and system availability**

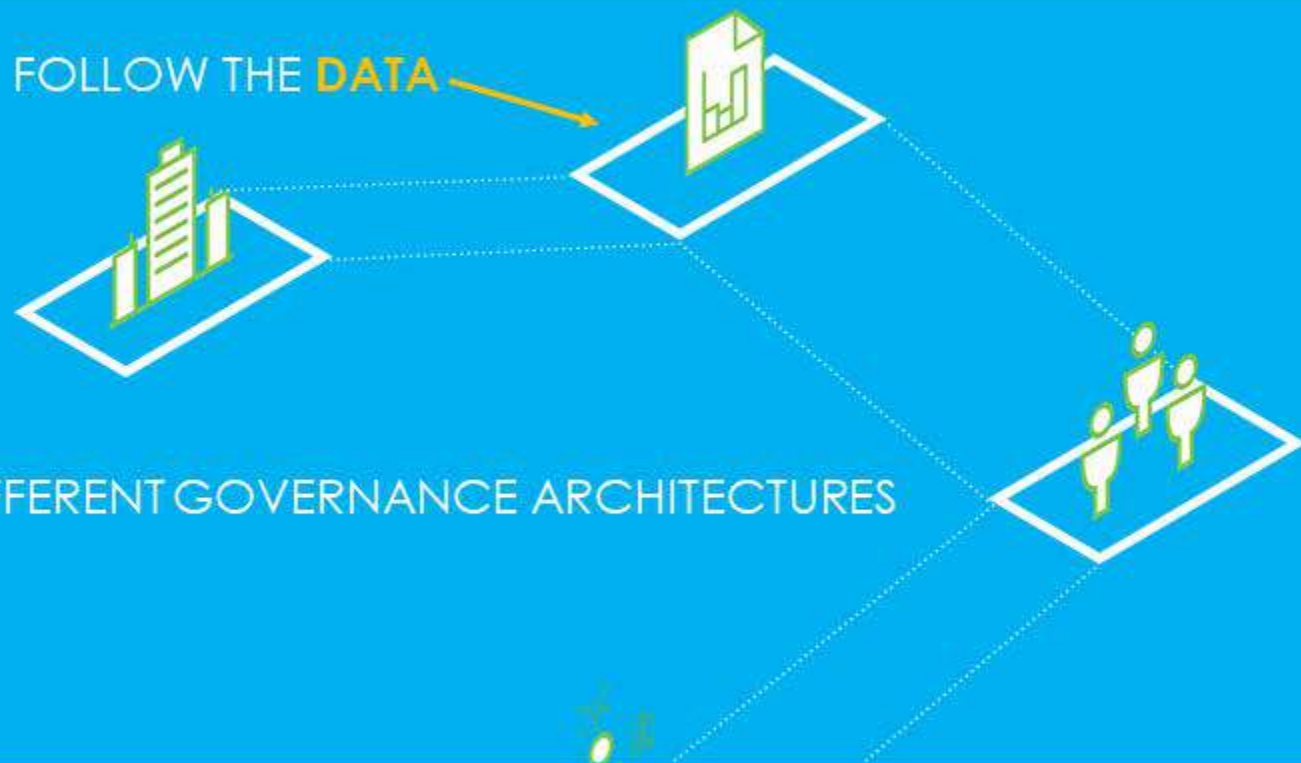


Annual savings exceeds \$10 million

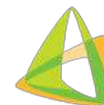


**Audit & Portability requests reduced from weeks to seconds even sub-seconds**

# Preparing for **GDPR**



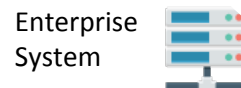
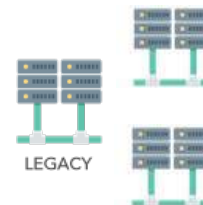
## REALITY CHECK: BUSINESS INFORMATION LANDSCAPES ARE COMPLEX AND MESSY



systemware



If it ain't  
broke don't  
fix it....

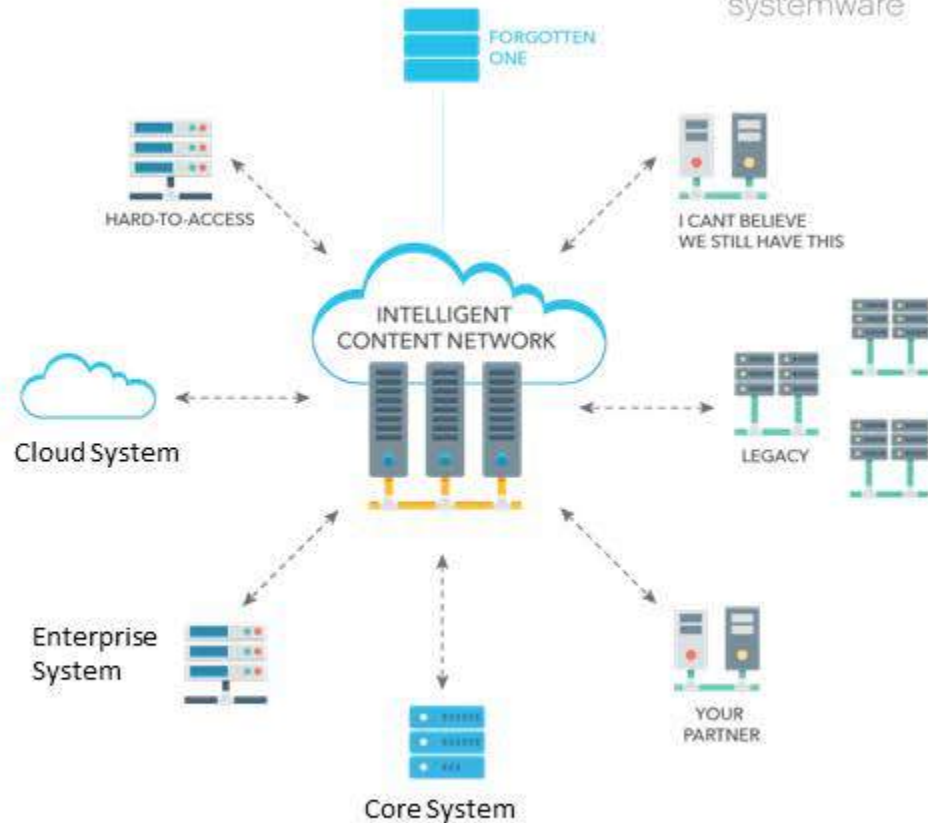


REALITY CHECK: BUSINESS INFORMATION  
LANDSCAPES ARE COMPLEX AND MESSY



systemware

Over 400 IM  
Systems Globally

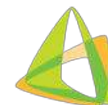




## Have a plan...

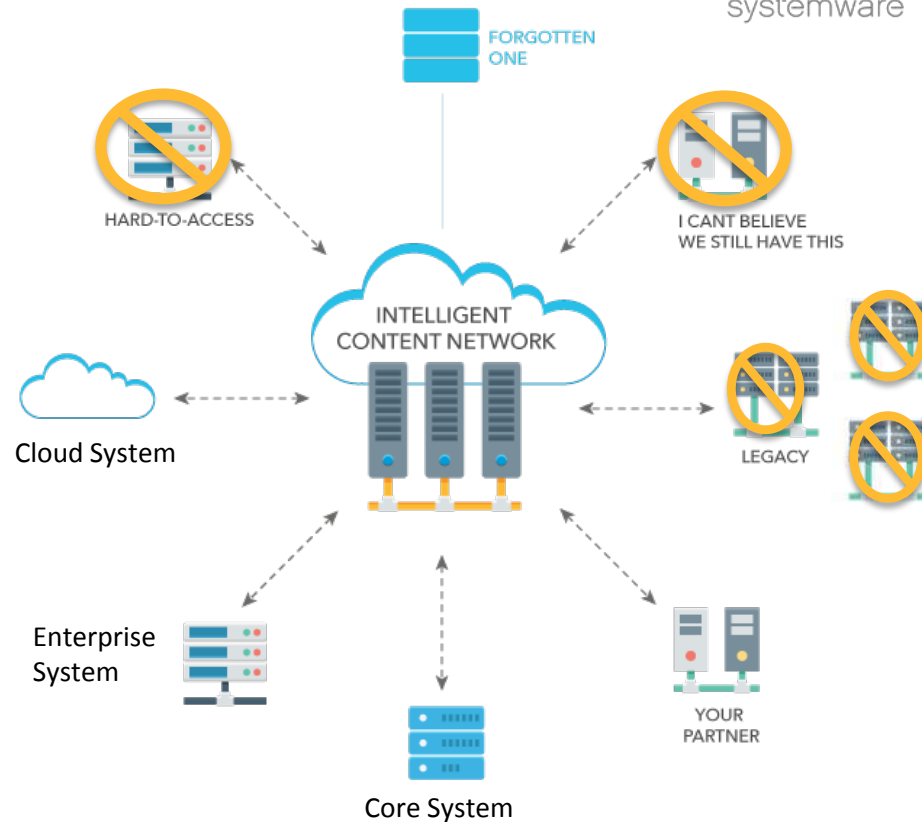
| Enterprise Class  | Underperforming  | Legacy  |
|---|--|---|
| Bidirectional Connectors with the Enterprise Class Go Forward Systems | Connect to storage of information in place on the current system and decommission once processes are in place. | Decommission legacy systems and migrate all information off existing legacy systems to new solution |
| GO FORWARD SYSTEMS  | LIMITED USE SYSTEMS  | HIGH RISK SYSTEMS   |

## REALITY CHECK: BUSINESS INFORMATION LANDSCAPES ARE COMPLEX AND MESSY



systemware

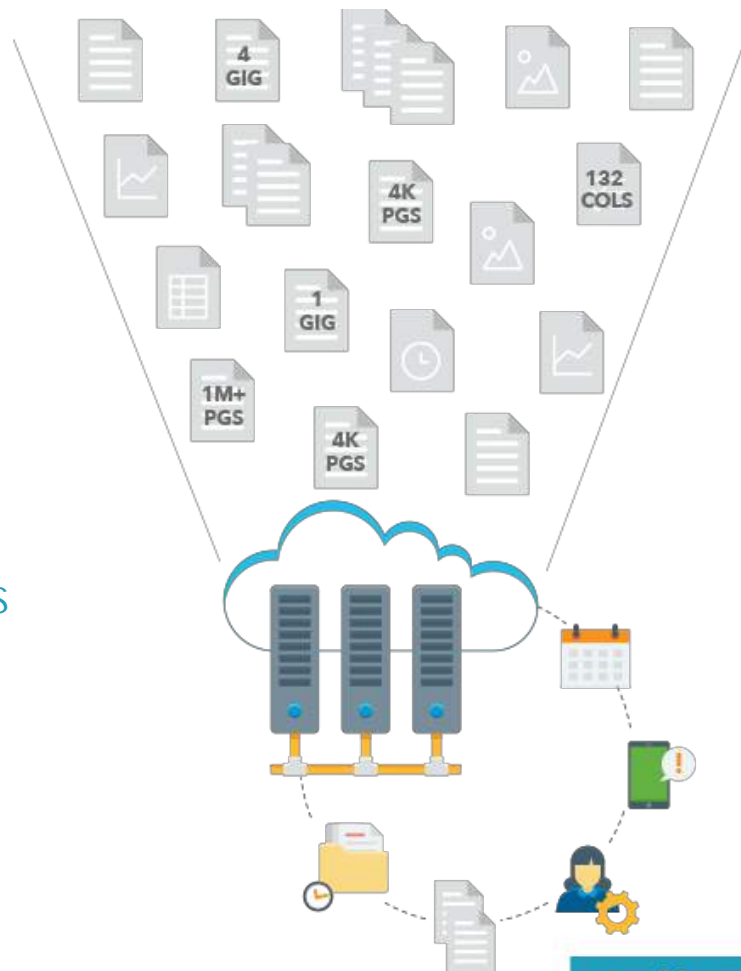
# Over 400 IM Systems Globally





## REALITY CHECK: BUSINESS INFORMATION LANDSCAPES ARE COMPLEX AND MESSY

- Encrypt data at rest
- Realize storage reduction of 90%
- Interrogate your information
- Do not disrupt end users and customers



# WHICH RULE?

**A SINGLE SET OF CRITERIA DOES NOT EXIST. CHALLENGES IN TRYING TO MAP TO ONE SET OF CRITERIA & WHICH HEIRARCHY STANDS.**



Dodd-Frank

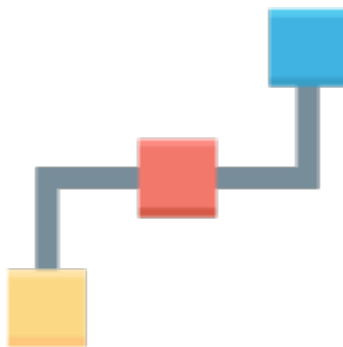


Gaming  
Regulatory Act



# Step back

# Which regulation requirements are the same or similar, and which are different?



Dodd–Frank



Gaming  
Regulatory Act



# MAP CONTROLS TO A REGULATION MATRIX

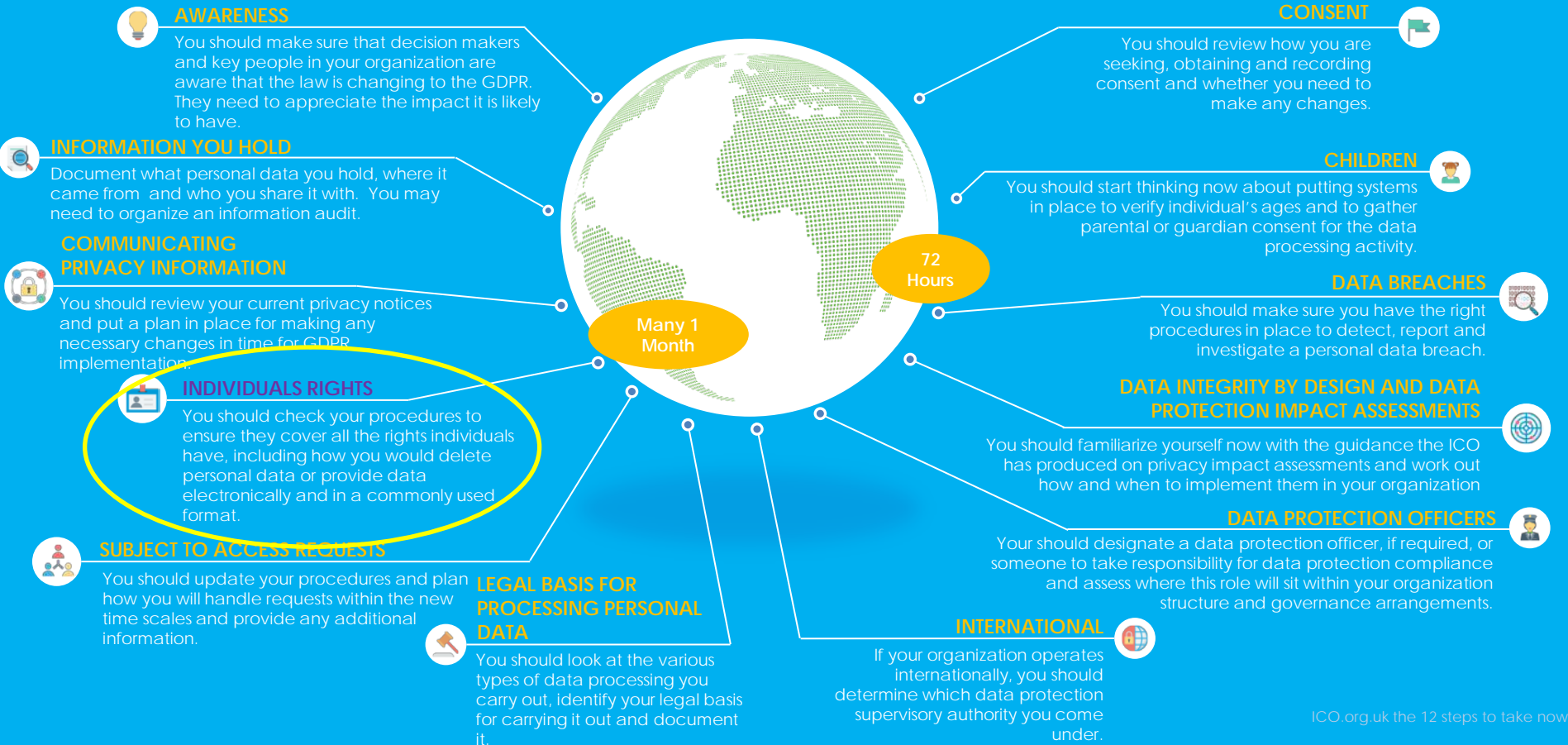


Dodd-Frank



Gaming  
Regulatory Act

# Preparing for GDPR



# Preparing for Compliance

## The Individual's Rights



to be informed



to rectification



to restrict processing



of access



to data portability



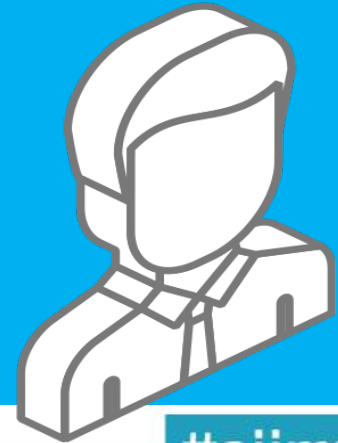
to erasure



to object



in relation to  
automated decision  
making and profiling



# ASSESS PROCESSES AND SYSTEMS





# USERS HAVE LEARNED TO BUILD PROCESSES AROUND LIMITATIONS



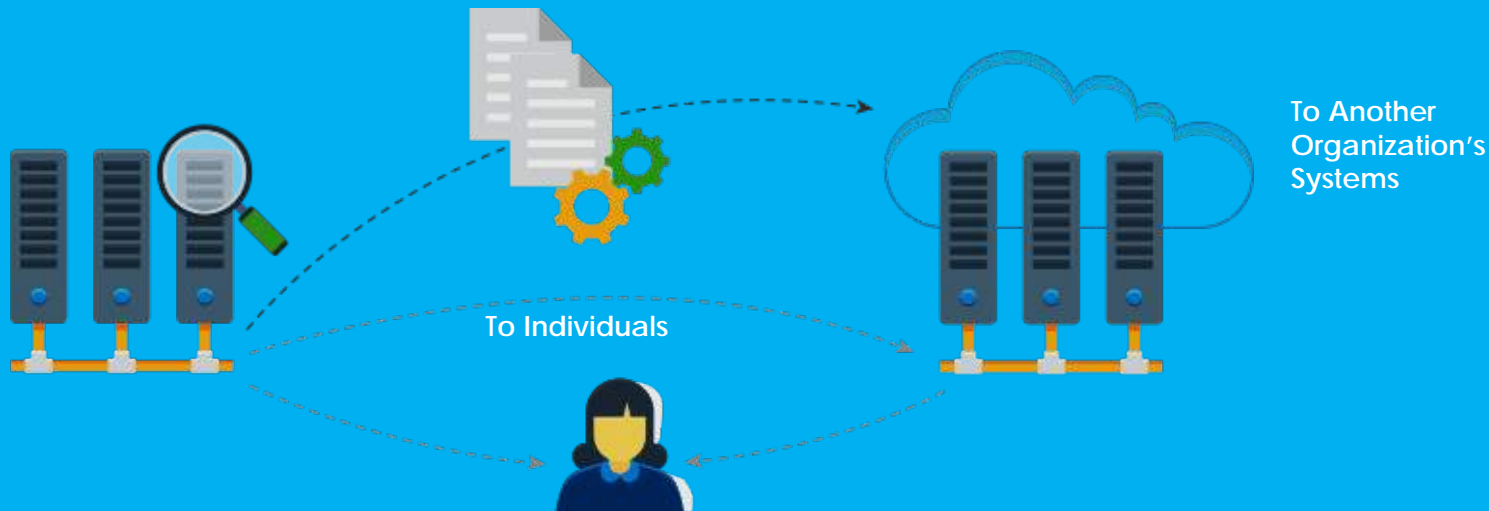
OUR ULTIMATE  
INTEGRATORS



# Preparing for **GDPR**

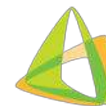
Data Portability

**DELIVER THE RIGHT INFO TO THE RIGHT PLACE**



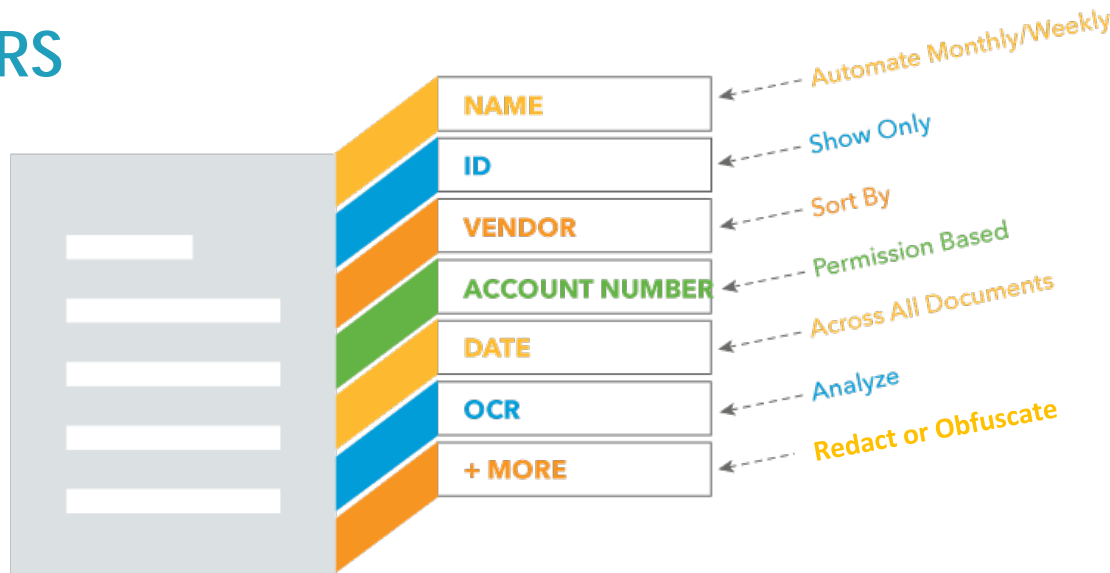
# Preparing for GDPR

## Meta Data



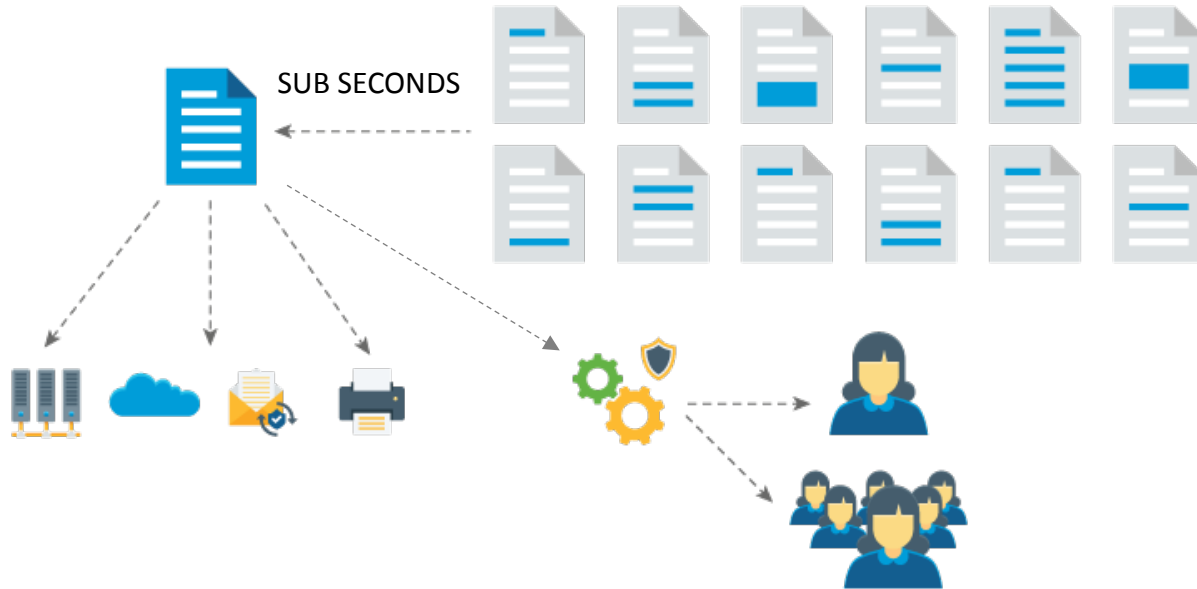
systemware

HAVING THE RIGHT  
META DATA MATTERS  
FOR NEW  
COMPLIANCE  
REGULATIONS



# Preparing for GDPR

## Data Portability



# OPPORTUNITY



- DATA MINING DIRECTLY OFF OF DOCUMENTS/AUTOMATION/SCRIPTING
- AMPLIFY BUSINESS REPORTING AND ANALYTICS
- CUSTOMER SELF-SERVICE

- **Connect Silos**
  - IDENTIFY THE GO FORWARD VS. LEGACY OR UNDERPERFORMING SYSTEMS
- **Ranking Regulations**
  - DEFINE REGULATION AND COMPLIANCE MATRIX TO FEED RISK ASSESSMENTS
- **User Processes**
  - INVOLVE CROSS FUNCTIONAL TEAMS LEGAL, BUSINESS, AND IT AS SOON AS POSSIBLE
- **Beyond Porting**
  - TAKE ADVANTAGE OF THE CAPABILITIES GDPR GIVES YOUR BUSINESS

# HOW TO REACH ME



## Andrea Chiappe

Director of Strategy & Innovation

Email: [Andrea.Chiappe@systemware.com](mailto:Andrea.Chiappe@systemware.com)

Twitter: @ChiappeAndrea



# Thank You To Our Sponsors





# Reynold Leming, Managing Director Informu Solutions Ltd



# Information Audit

What are we storing? How to Conduct an Information Audit of Personal Data and Content and Form an Action Plan

# Lots of Personal Data!

## What?

- Personal details, contact, profiling or ID
- Genetic and Biometric
- Criminal convictions, offences
- Education & training
- Employment details
- Financial details
- Health information
- Images, voice recordings
- IP address, Mobile Device ID

## Who?

- Children
- Complainants
- Consumers
- Contractors
- Customers
- Enquirers
- Funders
- Marketing Prospects
- Staff
- Suppliers
- Visitors

## Where?

- Document, messaging, AV, graphical, web, database content

### Across

- Corporate Physical Filing
- Offsite Archives
- Corporate Digital Estate
- Cloud
- Personal and Mobile Devices
- Suppliers, Partners, Outsourced Contracts

# The Need for an Audit



Preparing for the General Data Protection  
Regulation (GDPR) 12 steps to take now

2

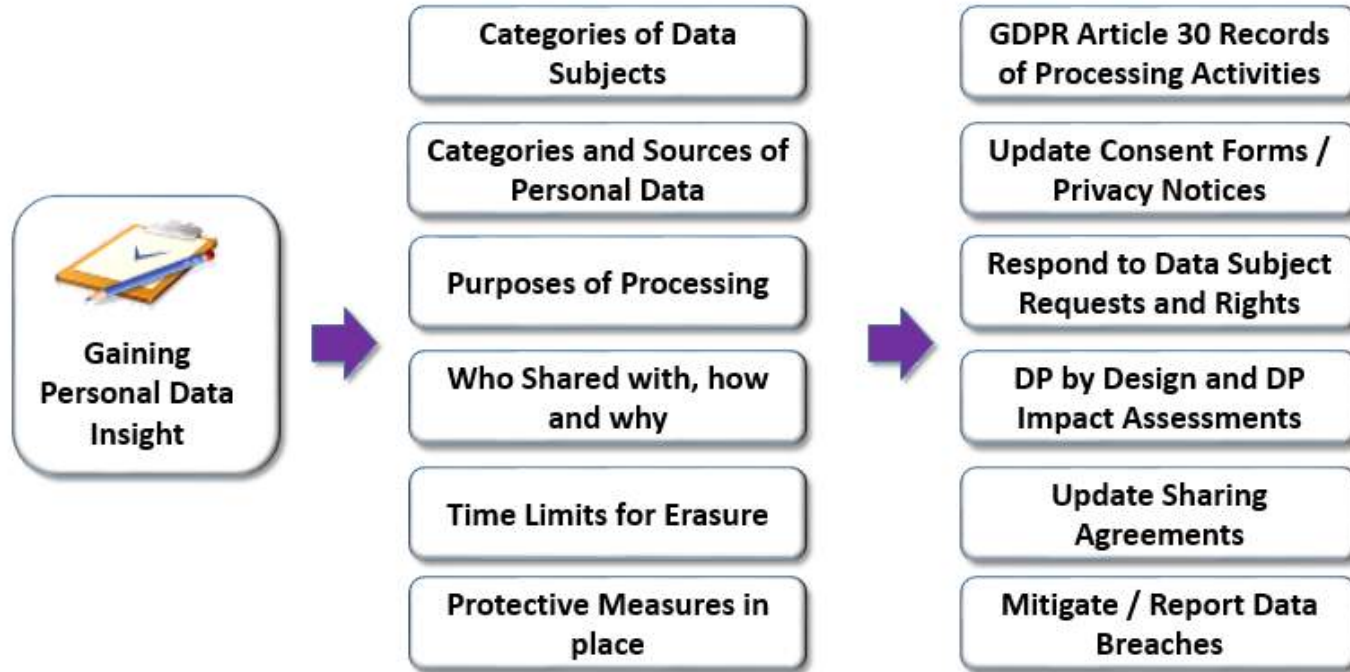
## Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

**Ensures activities involving personal data are identified for embedding Data Protection by design and default into business processes and systems**

**Ensures an organisation is accountable, transparent and can create the necessary records of processing activities for GDPR compliance**

# Questions and Answers



# Data About Personal Data

## Asset Data:

- Business Function & Activity
- Asset Name
- Description
- Asset Owner
- Asset Administrator
- Format
- Status
- Utilisation
- Data Repository
- Data Repository Owner
- Data Repository

Location Country

- Security Controls
- Business Continuity Controls
- Retention Rule
- Long Term Storage Location
- Disposal Method

## Personal Data:

- Personal Data Category
- Processing Reason
- Processing Condition
- Data Subject Type

• Data Subject Location

- Sensitive Personal Data?
- Data Elements Collected
- Last updated
- Number of PI Records
- Data Source
- When is data obtained?
- When is it updated?
- Data Accessors
- Means of Access
- Data Elements Accessed

• Purpose of Access

## Data Sharing:

- Sharing Status
- Shared With
- Sharing Agreement
- Purpose of Sharing
- How Shared?
- Data Elements Shared
- Shared Processing Location
- Processor Security Controls

# What is an Information Asset?

## The National Archives:

"Assessing every individual file, database entry or piece of information isn't realistic. You need to group your information into manageable portions"

"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively"

**Paper** – the file types maintained both onsite and at archive storage (for which there may be many instances within a series) and important individual documents, such as unique certificates / consents.

**Electronic Files** – ranging from, for example, an important individual control spreadsheet, to a whole collection of digital records sharing same profile and business purpose.

**System Data** – could be a whole database serving a single primary purpose or alternatively distinct sub sets of data within a line of business application that delivers a range of functionality (such as an ERP system).

# The Audit Process

## **Suggested steps to conducting the audit:**

1. Agree the questionnaire design, including scope of controlled lists within drop-down selections.
2. Identify the participants (information asset owners / administrators).
3. Conduct a pilot audit, subsequently refining the questionnaire.
4. Conduct a series of business seminars to introduce and explain the audit.
5. Self-audit by teams, with advisory resource available to support upon request.
6. Re-visits following initial audit as required of clarifications required.
7. Analysis of findings to identify both opportunity and risk.
8. Interviews and observation would be valuable if data mapping.
9. Use of file analysis tool if desired for deeper dive assessment of digital content.
10. Physical file / box inventory if required to catalogue legacy records.

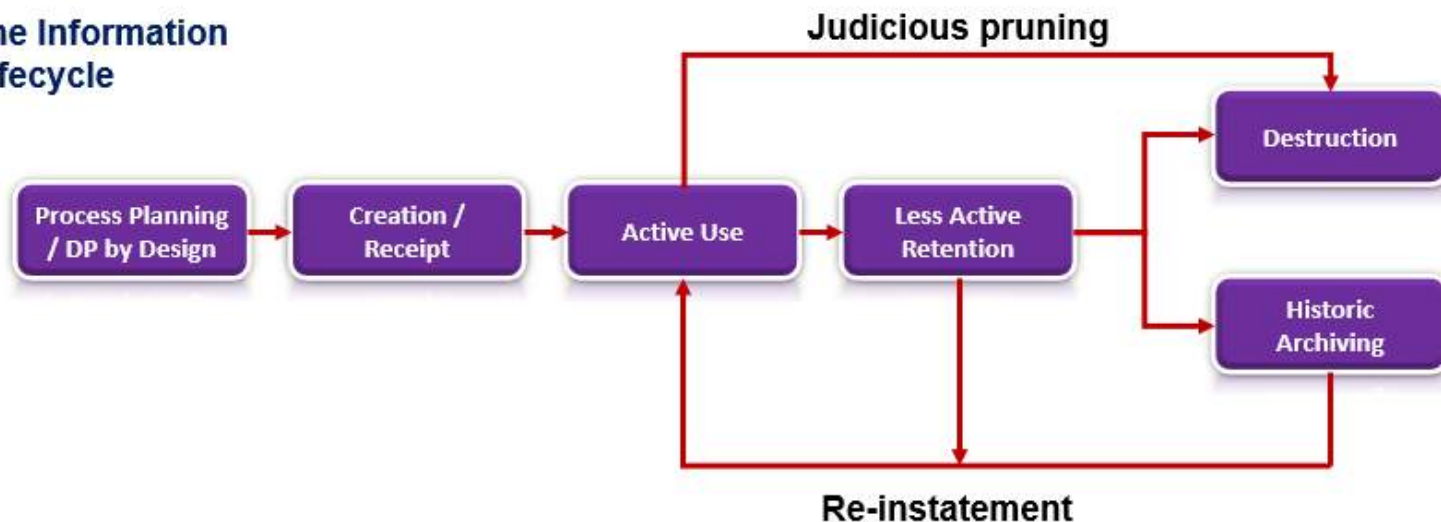


# The Outcome!

## Principles Applied



## The Information Lifecycle



# HOW TO REACH ME

- Reynold Leming
- Informu Solutions Ltd
- +44 (0)7966 397417
- [Reynold@informu-solutions.com](mailto:Reynold@informu-solutions.com)

# Marc Stephenson, CTO

## Metataxis



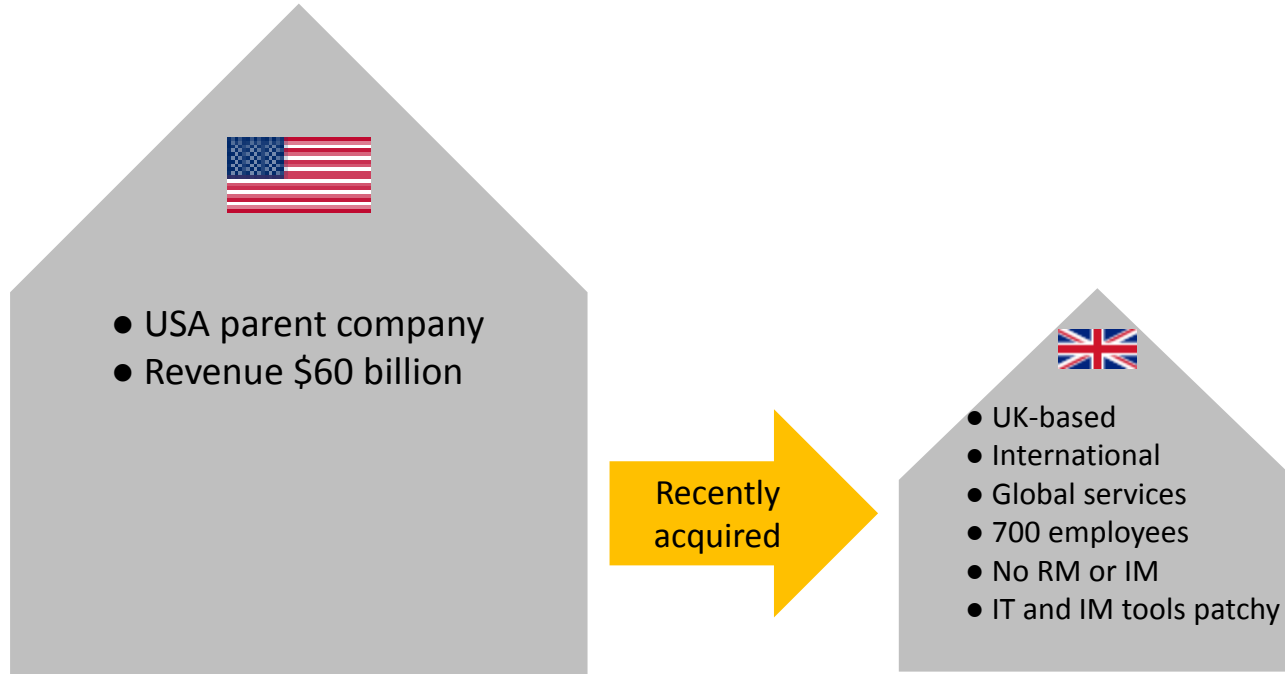
# Get Doing Privacy Right now!

A case study in implementing GDPR for a global services organisation

September 2017

## Metataxis

# The Organisation

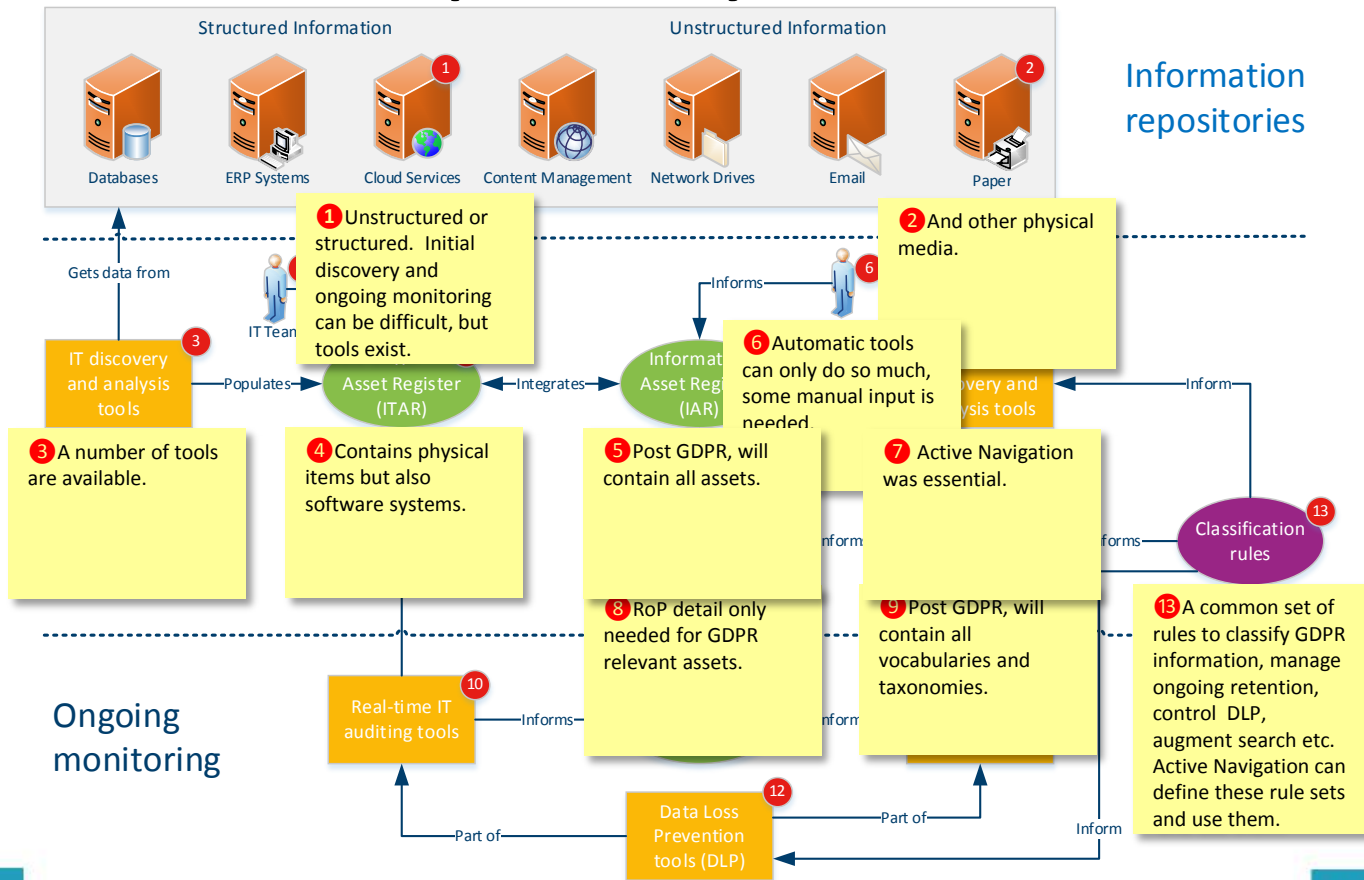


- Security audit revealed range of issues, including no GDPR programme
- Programme started to remediate and improve governance, incl. GDPR

# Steps Taken

- Parent company already supported by global law firm for **legal** GDPR issues
- Metataxis provided support on **information management** GDPR issues
- Aim was to meet the needs and concerns of Legal, IT and IM teams and translate them into **operational, practical** steps for GDPR compliance
- Additional aim was to provide the basis for wider IM and governance regime
- Needed extensive *file analysis* – significant volumes of unstructured information, so used Active Navigation (leaders in the space)
- A GDPR *capability architecture* was developed to operationalize the required steps, and identify the tools to achieve them

# GDPR Capability Architecture



# Diagram Key

1. Could be unstructured or structured. Discovery and real-time auditing can be difficult, but tools exist.
2. And other physical media.
3. A number of tools are available.
4. Contains physical items but also software systems.
5. Post GDPR, will contain all assets.
6. Automatic tools can only do so much, some manual input is needed.
7. Active Navigation was essential.
8. RoP detail only needed for GDPR relevant assets.
9. Post GDPR, will contain all vocabularies, taxonomies and maybe ontologies.
10. Monitor relevant activity and may detect immediate issues.
11. Most likely a collection of documents or evidence grouped by incident.
12. Generate alerts on data breaches.
13. A common set of rules to classify GDPR information, manage ongoing retention, control DLP, augment search etc. Active Navigation can define these rule sets and use them.
14. Could be an explicit system or a coordinated use of tools.



# Status and Next Steps

## Status

- Initial RoP complete – fields, taxonomies, some data
- Discovery phase complete – file analysis and structured analysis

## Next Steps

- A solution architecture to be created – a project in itself
  - Tools? Costs? Deployment? Integration? Configuration?
- Controlled vocabularies (taxonomies)
- Wider information architecture
- Information management policies and governance framework
- Retention and disposal schedules
  - Includes defensible deletion by Active Navigation
- Change management and training initiatives

# HOW TO REACH ME

## Metataxis



@Metataxis

Presenter, Metataxis  
Marc Stephenson, CTO

marc.stephenson@metataxis.com  
www.metataxis.com  
+44 (0)7870 345378



@ActiveNav

Active Navigation  
Patrick Cardiello, Marketing Manager

patrick.cardiello@activenavigation.com  
www.activenavigation.com  
1 (914) 262 6131

# Robert Perry, VP, Product Management ASG



# The Four P's of GDPR Readiness

Robert Perry  
Vice President, Product Management  
ASG Technologies

# Are You on the Path to GDPR Compliance?

What personal data is stored and how are we using it?

How is my organization affected by the GDPR?

What is our lawful basis for collecting personal data?

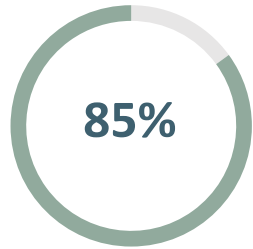
Do I need a Data Protection officer for compliance?

Are we making enough progress towards compliance today?



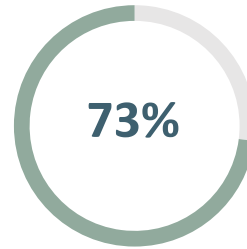
# GDPR Preparation is Underway but a Challenge

## Requirement for DPO is being met



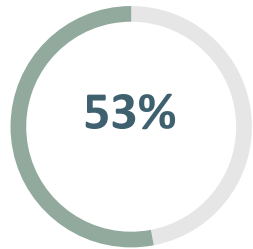
Have appointed Data Protection Officer<sup>1</sup>

## Private data is difficult to identify and sustain



Nearly ¾'s of respondents said private data is either very or somewhat difficult to identify or sustain<sup>2</sup>

## Preparation is moving forward in many companies<sup>2</sup>



A little more than half respondents feel very or somewhat prepared for GDPR<sup>2</sup>

## Few use systematic, organized approach for Privacy Impact Assessments<sup>1</sup>



Use automated system (in-house or commercial)



Have procedure or framework to identify and classify risk to individuals

### Sources:

1. Organisational Readiness for the European Union General Data Protection Regulation (GDPR), Center for Information Policy Leadership and Avepoint.
2. How to Tackle the Challenges of GDPR Readiness, The A-Team Group for Data Management Review. Commissioned by ASG Technologies

# Four P's of GDPR Compliance

**P**

**reparation:** educate teams and create baseline view of current data, business processes, and data flows that use personal data

**P**

**roduction:** adapt practices for data collection, data processing, application design within regulations

**P**

**erformance:** implement oversight and be prepared for supervisory audits, breach notification requirements

**P**

**ersistence:** use reporting to maintain compliance through monitoring and continued education and prove knowledge of data processed and how

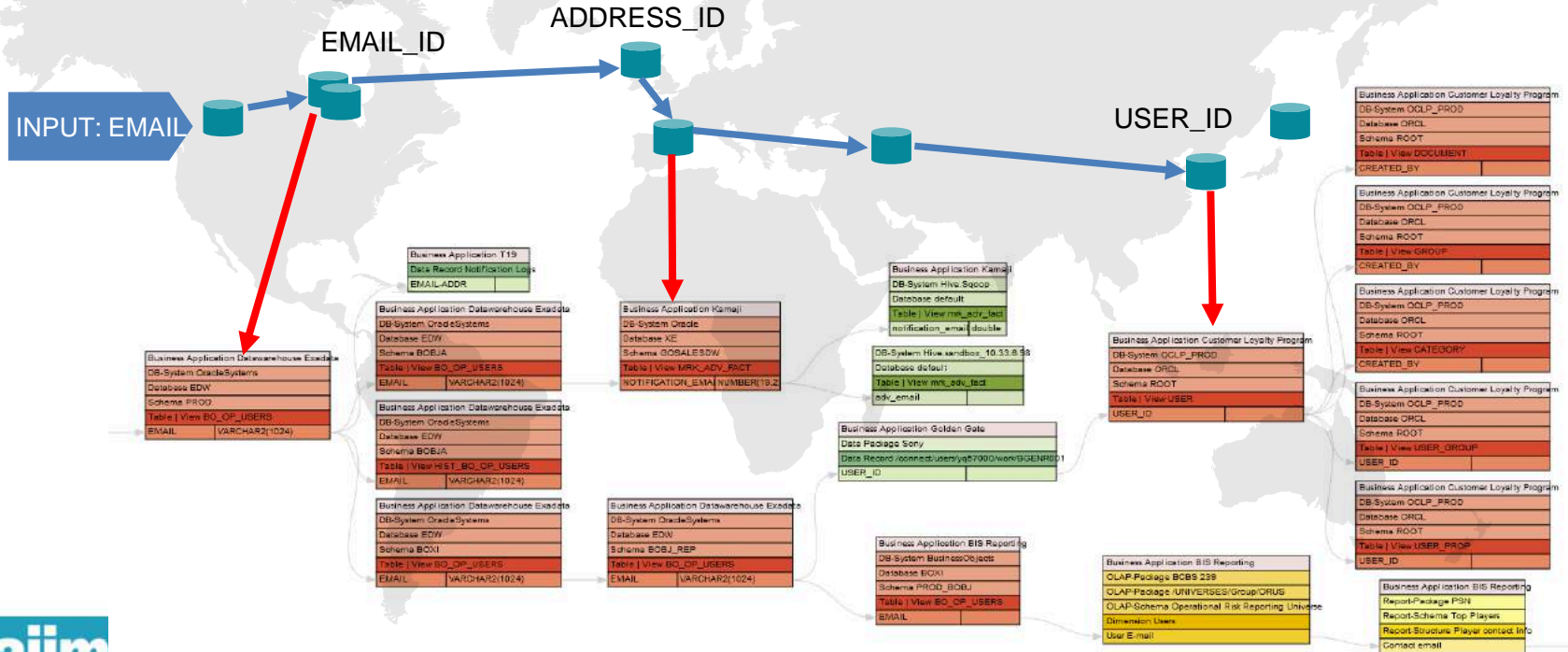
# Preparing for GDPR Compliance

| Action   | Implementation   |
|--|--|
| Education  | Internal training programs, certifications for staff handling personal data.   |
| Evaluate infrastructure  | Assure data governance, content management, data management capabilities can support new requirements for archival, records, processes and data management |
| Identify personal data currently stored; how you got it; and business processes it touches | Inventory data and application estates to know data is stored and what processes use it. Delete unused data where no lawful basis for use exists.          |
| Determine lawful basis for processing personal data  | Review the ways to lawfully collect data, determine which is appropriate for private data collected and document for supervisory authorities if asked.     |
| Update processes for gaining consent   | Assure all forms include language for consent when consent is lawful basis. Determine how to capture and store consent.                                    |
| Appoint Data Protection Officer  | Determine if needed and if so, hire. Establish roles throughout organization.  |
| Prepare for data breaches  | Organize process for identifying breached data and all affected individuals  |
| Build processes with privacy by design   | Establish approach to data collected, anonymize as possible, review processing and data transfers with goal to minimize and consider security of data.     |



# Identifying Personal Data

“WHERE IS ALL PERSONAL DATA?”



# ASG Solutions for Compliance

## Zero-Gap Data Lineage



Identify location of private data across enterprise

## Transparent Data Flow Visualization



Understand data source and destination and how processes manipulate it

## Policy-based data management



Manage all content types with encryption, archiving, redaction and deletion

## Standards-based APIs



Integrate with extended compliance ecosystem

## Comprehensive Metadata and Content Repositories



Maintains mapping of data estate and manages content lifecycle in compliance with regulations

## Robust Data Governance



Issue management, tracking and status dashboards for audit ready environment

# HOW TO REACH ME

Robert Perry

Vice President, Product Management

[rob.perry@asg.com](mailto:rob.perry@asg.com)

# Paul Lanois, VP & Senior Legal Counsel Credit Suisse



# EU's General Data Protection Regulation: How will this impact how you manage information in your organization?



Paul Lanois, LL.M.

Global Data Privacy and Technology Lawyer

Fellow of Information Privacy, CIPP US/C/E/A, CIPM, CIPT, PCIP

Vice President and Senior Legal Counsel, Credit Suisse

# Paul Lanois, CIP, FIP, CIPP



Paul.lanois@outlook.com

Paul is a global privacy, data protection and information security law expert. He is Vice President and Senior Legal Counsel working at a leading international bank (Credit Suisse) and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He has spoken at numerous conferences across Europe, the United States and Asia.

He received the 2017 AIIM Leadership Social Buzz at the AIIM Conference 2017. He was also named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. In addition, he was recognized as a leading lawyer in The Legal 500's GC Powerlist and was awarded the 2017 Advocacy Award from the Association of Corporate Counsel (ACC).

He has been recognized as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C). He is a Certified Information Professional (CIP), a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Technologist (CIPT). He also holds certifications in information security, including the CCSK, PCIP, CISMP, SSCP and Security+.

**Note: the views expressed are mine alone and do not necessarily reflect the views of my employer.**

# The GDPR

- The EU Commission presented its proposal in January 2012 as a replacement of the Data Protection Directive 95/46.
- After negotiating with the EU Council, the draft GDPR was adopted by the European Parliament on April 14th 2016 and published on May 4th 2016 in the EU Official Journal.
- The GDPR entered into force 20 days after its publication in the EU Official Journal.
- Its provisions will be directly applicable in all Member States two years after this date.

# Impacts of the GDPR

- **Increased enforcement powers:**

Previously, fines vary by Member State, and are comparatively low (ICO maximum fine is 500k GBP). The GDPR will significantly increase the maximum fine to €20 million, or 4% of annual worldwide turnover, whichever is greater. In addition, national data protection supervisory authorities are expected to coordinate supervisory and enforcement powers across the Member States, likely to lead to a more pronounced enforcement impact and risk for businesses.

- **Expanded territorial scope:**

Non-EU businesses will be subject to the GDPR if they: (i) offer goods or services to persons within the EU; or (ii) monitor the behavior of persons within the EU.

**Many non-EU businesses** that were not clearly required to comply with the Directive **will be required to comply with the GDPR.**



# Personal Data

- ‘Personal Data’ means any information relating to an identified or identifiable natural person (‘data subject’); 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.
- The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible.

# GDPR Action Plan

- Ensure the support from the board & business units
- Establish inventory of personal information held
- Privacy Notice & Information
- Individuals' rights
- Data subjects' access requests
- Data protection impact assessments (DPIA)
- Consent
- Children
- Personal data breaches
- Security of data processing & data protection by design
- Data protection governance

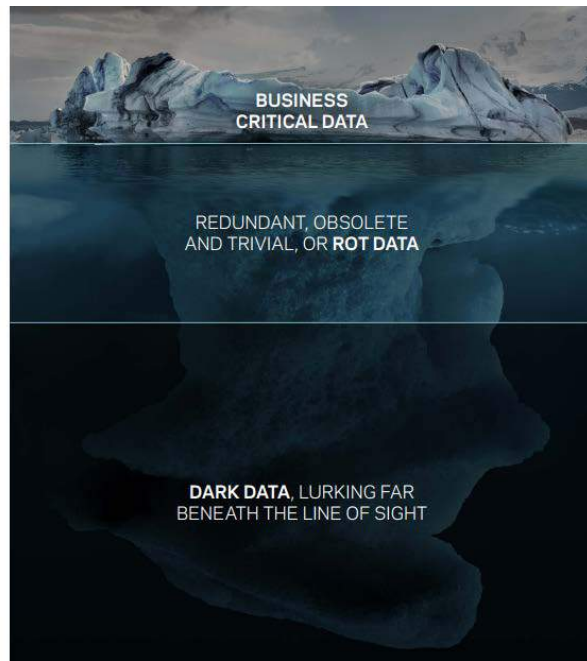
# Stakeholder Support

- Decision makers and key people in your organization must be aware of their accountability and appreciate the impact GDPR is likely to have so that they can identify areas and processes that will need to change.
- Implementation could require significant resources, especially for larger and more complex organizations.

# Inventory of Personal Information

You should document:

- what personal data you hold
- where it came from and
- who you share it with



# Privacy Notice & Information

You must give notice that:

- Provides details of the grounds that are used to justify processing
- highlights that consent may be withdrawn, the existence of the data subject rights and the right to lodge a complaint with the Supervisory Authority, and
- is concise, transparent, intelligible and in an easily accessible form using clear and plain language.

# Individuals' Rights

The main rights for individuals under the GDPR will be:

- access to their personal data,
- to have inaccuracies corrected,
- to have information erased,
- to object to the processing of personal data for direct marketing purposes,
- to prevent automated individual decision-making and profiling, and
- data portability.

# Data Subjects' Access Requests

- Data subjects will have a right to request a copy of their personal data undergoing processing. They may also request:
  - the purpose of processing, the period of time for which data will be stored, any recipients of the data, the logic of automated decision-making, including profiling, and the envisaged consequences of any such processing.
- The controller must take the appropriate action “without undue delay” or at the latest within a month of the request.

# Privacy Impact Assessments

- The GDPR introduces Data Protection Impact Assessments (DPIA) as a means to identify and deal with high risks, notably to the privacy rights of individuals when processing their personal data.
- The DPIA requirement is linked to processing “likely to result in a high risk for the rights and freedoms of natural persons,” taking into account “the nature, scope, context and purposes of the processing.”



# Consent

- Consent must be “freely given, specific, informed and unambiguous.”
- Consent has to be specific to the processing operations. The controller cannot request open-ended or blanket consent to cover future processing.
- GDPR requires the data subject to make a statement or clear affirmative action removing the possibility of “opt-out” consent or the interpretation of silence, inactivity, and pre-ticked boxes as a means of providing consent.

# Children

- GDPR introduces specific protections for children who are identified as “vulnerable individuals” and deserving of “specific protection”. This applies to children under the age of 16, unless a Member State has made provision for a lower age limit (lowest age limit is 13).
- Where online services are provided to a child and consent is relied on as the basis for the lawful processing of his or her data, consent must be given or authorized by a person with parental responsibility for the child.

# Personal Data Breaches

- A “personal data breach” is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
- In the event of a personal data breach, as a general rule, data controllers must notify the supervisory authority.
- Notice must be provided “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” If notification is not made within 72 hours, the controller must provide a “reasoned justification” for the delay.

# Security & Data Protection

- Controllers and processors are required to “implement appropriate technical and organizational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.”

# Data Protection Governance

- GDPR requires all organizations to implement a wide range of measures to reduce the risk of contravening GDPR requirements and to prove that they take data governance seriously.
- Accountability measures include: Data Protection Impact Assessments, audits, policy reviews, keeping records of processing activities and (potentially) appointing a Data Protection Officer (DPO).
- For those organizations which have not already allocated responsibility and budget for data protection compliance, these requirements will impose a heavy burden.

— **THANK YOU** —

Paul Lanois, Credit Suisse

# Theresa Resek, CIP, Director AIIM



# What GDPR Means for US Companies

Common Questions  
Non-EU Businesses are Asking



# How do I know if I need to worry about GDPR compliance?

- The rules follow the data
- US companies that are not located in the EU but do offer goods or services to EU citizens must be in compliance with GDPR
- Employee data for employees in the EU

# Are the fines the same for US Companies?

- Yes – EU regulators can fine US companies for violating GDPR, and they can do it with the help of US authorities
- Yes – this also applies to companies based in any other region of the world
- Penalties/fines (calculated on the company's global annual turnover of the preceding financial year) of up to 4% for non-compliance with the regulation

# HOW TO REACH ME

- Theresa Resek, CIP, AIIM
- [tresek@aiim.org](mailto:tresek@aiim.org)
- [@theresaresek](https://www.linkedin.com/in/theresaresek)
- [@tmressek](https://www.linkedin.com/in/theresaresek)
- [www.aiim.org/webinars](http://www.aiim.org/webinars)
- [www.aiim.org/podcast](http://www.aiim.org/podcast)

# Thank You To Our Sponsors



# GDPR is set to launch next year. Are you ready?

*FREE Report*

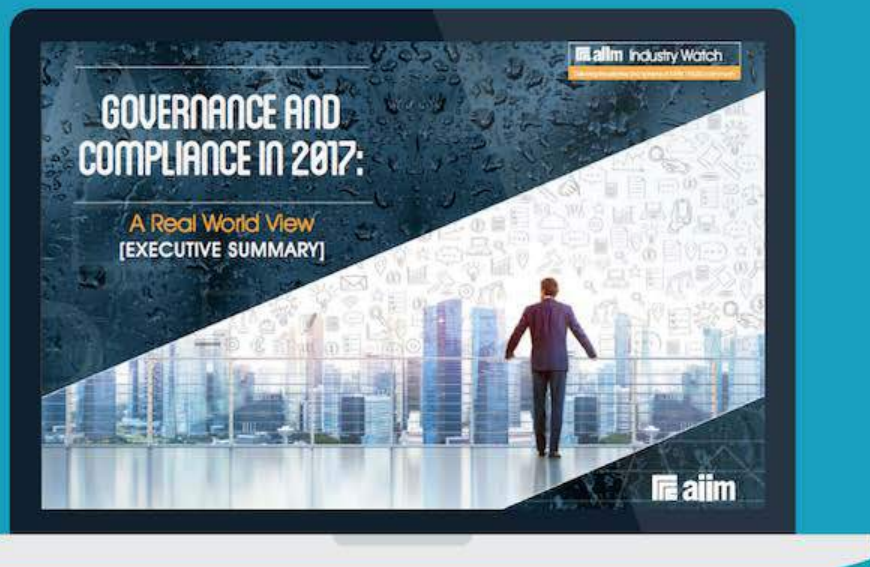


GDPR will have an international impact on how you manage and protect EU citizen-related information and data assets. Lack of compliance could lead to fines of up to 4% of revenue.

**Learn what you can do to prepare >**

[info.aiim.org/understanding-gdpr-readiness-in-2017](http://info.aiim.org/understanding-gdpr-readiness-in-2017)

# FREE REPORT: Get the real story of Governance and Compliance in 2017!



Stricter regulations including GDPR are demanding businesses to implement more focused information governance (IG) policies, practices, and enforcement efforts.

Download this study to explore how organizations are addressing their governance and compliance challenges.

[Click here to learn more >](#)

[info.aiim.org/governance-and-compliance-in-2017-a-real-world-view](http://info.aiim.org/governance-and-compliance-in-2017-a-real-world-view)

— **THANK YOU** —