GDPR: New Legislation

A Members Owned Not-for-Profit Organisation

Ray Ford
GDPR Consultant
CTO AISGroup plc

Founder Member of the GDPR Institut

A Members Owned Not-for-Profit Organisation

Agenda

- Introductions
- GDPR Overview
- GDPR Help Available and how you and your organisation can contribute to the GDPR Community
- GDPR Question and Answer session later

© 2017 - The GDPR Institut - All Rights Reserved

Introductions

- Who am I ?
- Why have I come here today ?
- Raise awareness on the impending GDPR legislation and hopefully assist you in determining what impacts it will have on your organisations?
- Provide a high level overview of some of the salient changes that will impact organisations handling private and sensitive data on EU citizens.
- Provide the opportunity for a Q&A session later and introduce the Institut as a source of assistance for organisations seeking advice on addressing this legislation?

© 2017 - The GDPR Institut - All Rights Reserved

GDPR Overview

A Members Owned Not-for-Profit Organisation

Regulation Impact

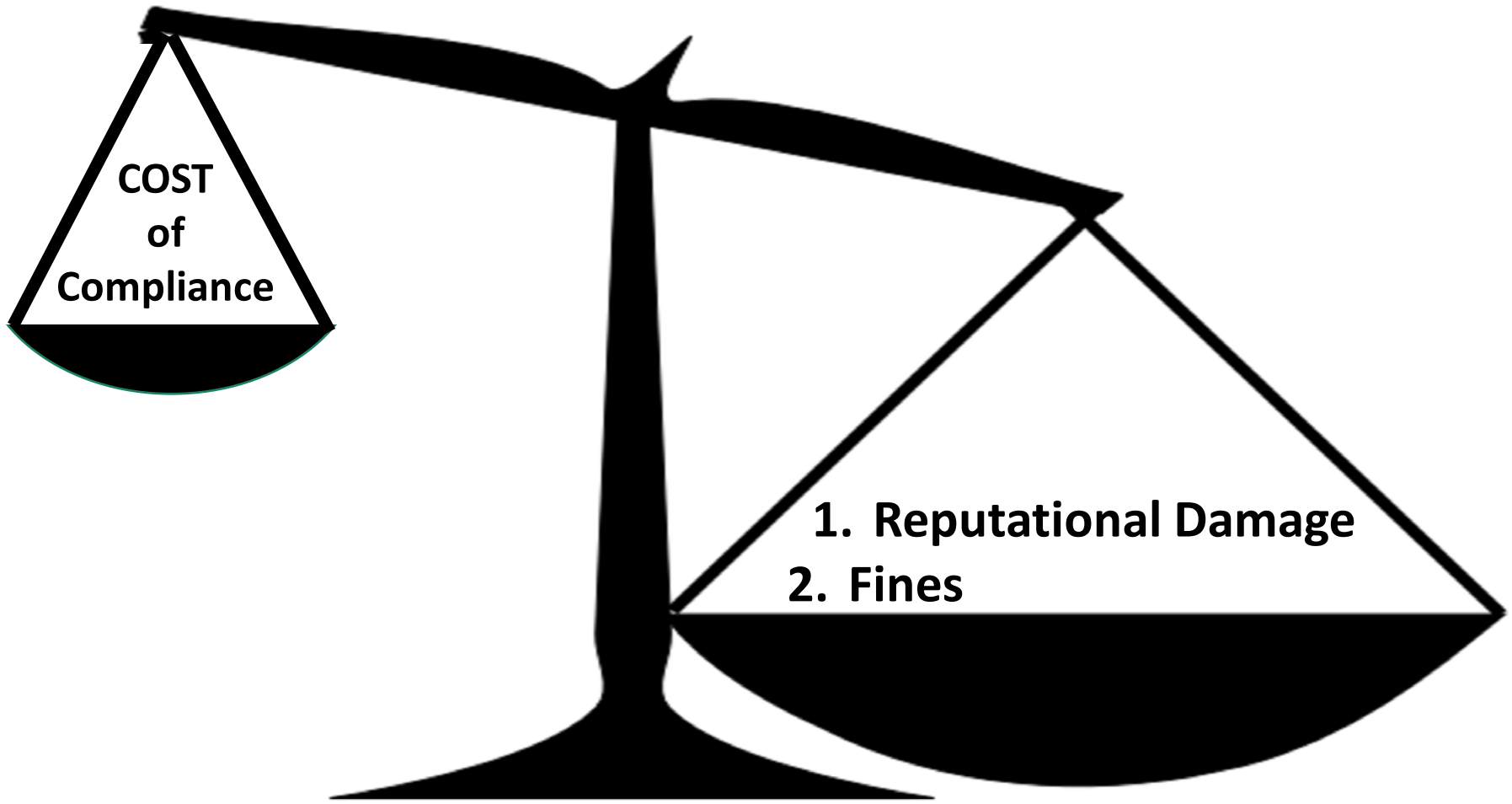
Do you control or process personal data about
ANY EU Citizens?

– including **Customers/ Patients** **Employees**
Suppliers

If so you have to be GDPR compliant by 25th May 2018 or manage the implications of failing to comply with the legislation requiring protection of PII data.

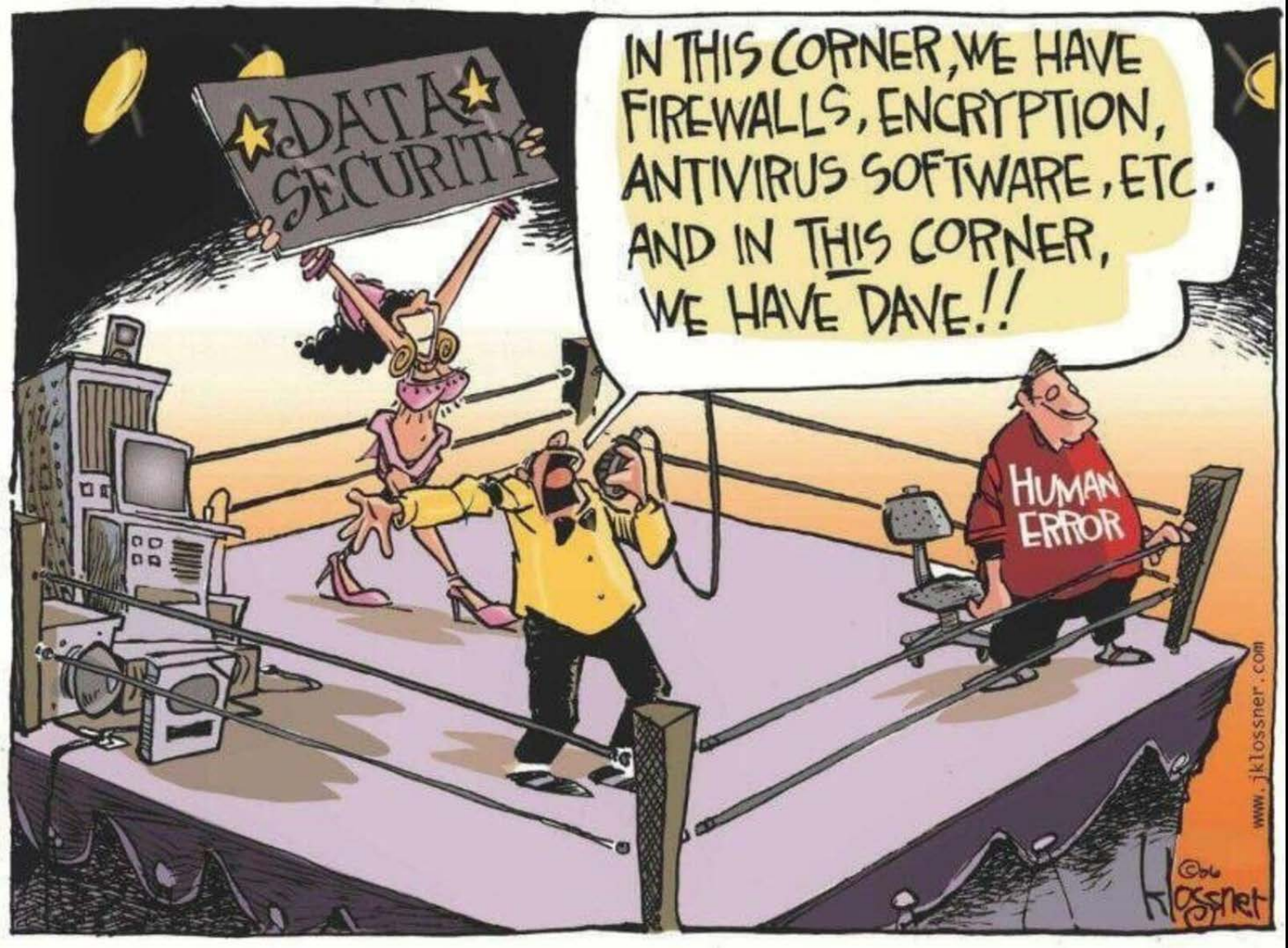
© 2017 - The GDPR Institut - All Rights Reserved

Opportunity or Challenge?



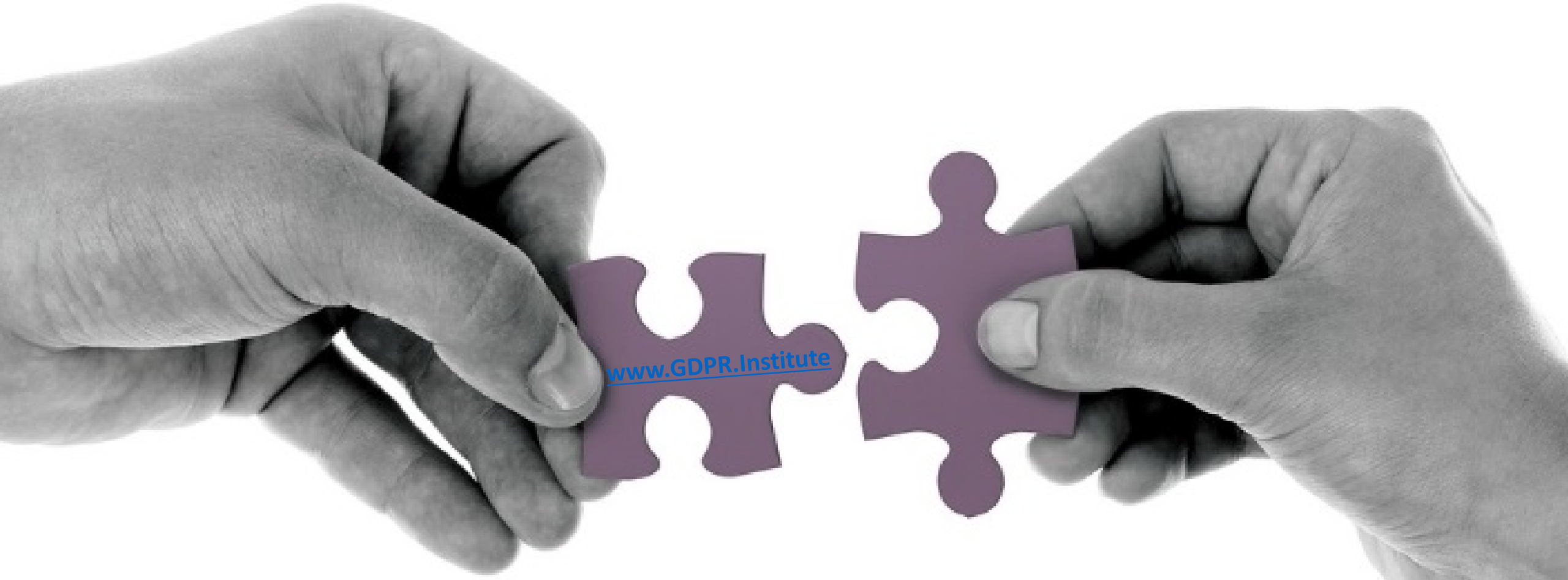
© 2017 - The GDPR Institut - All Rights Reserved

You will suffer a Data Breach at some time!



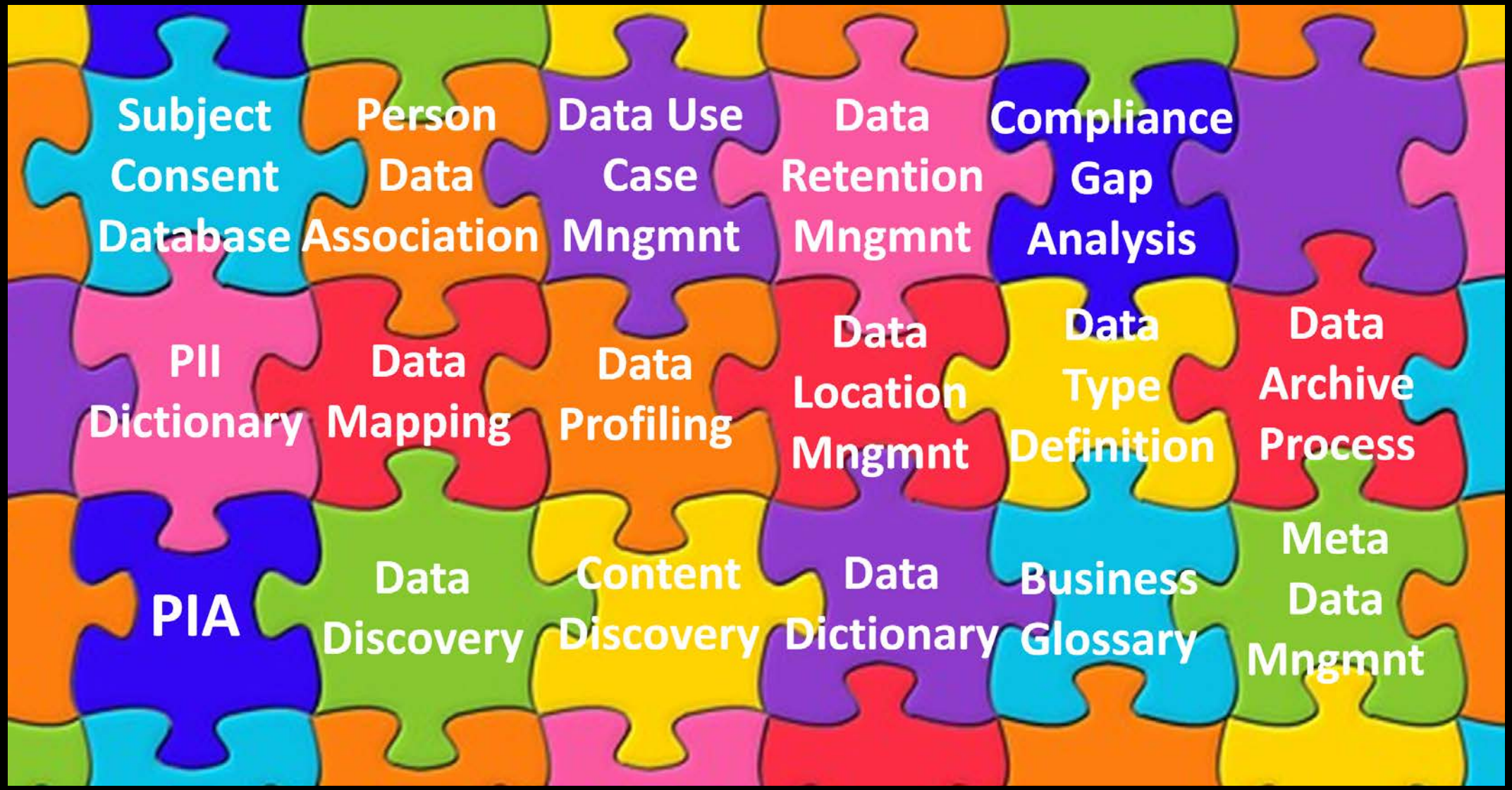
© 2017 - The GDPR Institut - All Rights Reserved

The “General Data Protection Regulation” Puzzle



Can you see the full picture and have you got all the pieces?

Understand your GDPR Landscape



© 2017 - The GDPR Institut - All Rights Reserved

Key Questions

1. What Personal Data do you hold? – Customer, Employee, Supplier, Contractor, Sub-Contractor, Citizen, Member, Pupil, Student, Patient etc

2. Where is that Data Located? - PC hard drive, Remote Storage or Backup Device, On Premise Database or Content Server, in “The Cloud”, Application Silo?

3. How are you using that Data? Is it shared?

4. Do you have Explicit or Implied Permission to use the data in the way you are using it?

© 2017 - The GDPR Institut - All Rights Reserved

GDPR Key Focus Areas

1. Privacy by Design – Enterprise Change
2. Your Data Protection Officer
3. Consent Management
4. Types of Data
5. Data Subject Rights
6. Data Subject Access Rights Management
7. Data Controllers & Data Processors
8. Implications of GDPR
9. Legal Changes
10. Contractual Implications

© 2017 - The GDPR Institut - All Rights Reserved

Immediate Action Plan

1. Seek Legal Advice
2. Conduct a Privacy Impact Assessment
3. Complete a Readiness Assessment to address the key questions
4. Secure Executive Sponsorship and a meaningful budget
5. Develop a Consent Management Strategy
6. Build a Data Subject Access Request process before you get swamped
7. Ensure you have all your Breach Detection technology in place – Database, Content Repositories, Network Traffic, Dark Web
8. Prepare for the worst, and breathe a sigh of relief if it doesn't happen

© 2017 - The GDPR Institut - All Rights Reserved

Everything YOU need for GDPR

A Members Owned Not-for-Profit Organisation

www.gdpr.institute

The GDPR Institut

Helping you resolve YOUR GDPR Challenge
& Maximise the GDPR Opportunity

A Members Owned Not-for-Profit Organisation

The Instituts' Purpose

Create a community of Data Privacy, Data Security and Data Governance experts to assist Large, Medium and Small Organisations address the challenge and maximise the opportunity created by the General Data Protection Regulation

GDPR Challenge

Or

GDPR Opportunity

© 2017 - The GDPR Institut - All Rights Reserved

Privacy by Design

1. Does your organisation have a defined published GDPR compliant privacy policy?
2. Are all your Databases Private by Design?
3. Are all your Content repositories Private by Design?
4. Are all your mobile devices secure and encrypted?
5. Are all your processes defined and audited/auditable but not data specific?
6. Is your Network Private by Design?
7. Are all your partners / data sharing network Private by Design?

© 2017 - The GDPR Institut - All Rights Reserved

The role of the Data Protection Officer

A Members Owned Not-for-Profit Organisation

The role of the DPO

1. You are legally required to employ a DPO, or the services of a DPO, if you are a public sector body or you are processing large quantities of person related data
2. The DPO is a regulatory only role
3. The DPO can have no operational responsibilities within your organisation
4. It is the responsibility of the DPO to report all Data Breaches to the regulator and all affected parties within 72 hours of it being detected
5. The role of DPO is a protected occupation, they cannot be dismissed for doing their job
6. The DPO is a senior role and should report at board level

© 2017 - The GDPR Institut - All Rights Reserved

Consent Management changes

1. Consent expires
2. You cannot have blanket consent any longer
3. The Data Subject has to take affirmative actions to give consent
4. The Data Subject has to be given choices
5. Consent has to be respected
6. Consent has to be managed
7. Consent has to be provable and auditable

© 2017 - The GDPR Institut - All Rights Reserved

The Rights of the Data Subject

1. Right of Transparency
2. Right of Access
3. Right to be Explained
4. Right to be Corrected
5. Right to be Reprocessed
6. Right to be Reprofiled
7. Right of Portability
8. **RIGHT OF ERASURE or RIGHT TO BE FORGOTTEN**

© 2017 - The GDPR Institut - All Rights Reserved

DSAR Management

- Data Subjects have the right to request access to the data you hold about them on a “reasonable frequency”
- You have 30 days to respond in full to each request
- Unlike the Data Protection Act, your organisation cannot levy a fee for providing the information about what data you hold about the Data Subjects to the Data Subject
- If you don’t respond at all, or respond in full, the Data Subject has the right to bring a private prosecution against your organisation and that prosecution will be supported by the regulator
- Have your DSAR Management process clearly defined, owned and a team ready to manage the flood of requests – this will be the new PPI

© 2017 - The GDPR Institut - All Rights Reserved

Positive Benefits of GDPR

Doing GDPR correctly has many positive benefits

- Enhanced Reputation
- Trusted Agent
- Defining the standard that competitors have to achieve
- Increased customer satisfaction
- Reduced data administration/DSAR

© 2017 - The GDPR Institut - All Rights Reserved

Negative Implications of GDPR

A Data Breach has very far reaching implications

- Punitive Fines
- Reputational Damage
- Increased inspection profile
- Regulator audits

© 2017 - The GDPR Institut - All Rights Reserved

Legal Changes

1. Fines
    - 4% of Global Turnover or €20m whichever is the greater
2. Consent Management
    - Consent Expires
3. Data Subject Rights
    - Lots of changes
4. Timescales
    - DSAR 40 days to 30 days (cant charge a penny)
    - Reporting from “sometime in the future” down to 72 hours
5. Implications for Data Controllers and Data Processors
    - Many changes – contracts, use cases, permissions, etc etc

© 2017 - The GDPR Institut - All Rights Reserved

www.gdpr.institute

Summary

A Members Owned Not-for-Profit Organisation

Summary

- GDPR is a very good thing
- GDPR sets a minimum standard for the use of personal data in the digital world
- GDPR focuses on Trust – creating, building, enhancing and maintaining personal trust in your organisation
- GDPR places the control of the persons data back with the Data Subject
- Do GDPR well and your organisation with soar, do it badly or not at all and implications are very grave
- Help is available, nobody has successfully completed a full GDPR Programme before. Trust nobody who claims to be an expert – its not possible!
- Seek advice from anyone and everyone
- **Join the Institute**

© 2017 - The GDPR Institut - All Rights Reserved

www.gdpr.institute

Membership

https://www.gdpr.associates/register/subscribe/

Help Line

+44 (0) 208 133 2545
contact@gdpr.institute

A Members Owned Not-for-Profit Organisation