WISDOM OF CROWDS

COLLABORATE | CREATE | DISTRIBUTE

ARCHITECTING THE GDPR-READY ENTERPRISE

THE EUROPEAN ADDENDUM

NOVEMBER 2017 - BRUSSELS

CHECKLISTS, MIND MAP & POLL RESULTS

CYBER MANAGEMENT ALLIANCE

Innovative Business Growth Platforms

WISDOM OF CROWDS

CONTENTS

EVENT SPONSORS

Platinum Sponsor

e2e assure

Gold Sponsor

advanced cyber solutions

Silver Sponsors

Jirasek security

SHIELDOX

VIGITRUST

HumanFirewall.io

netconsent Automating Compliance

GRC-ISMS plus

CONTRIBUTORS

Philippe Vandenborre, **Abbvie**
Sebastian Rohr, **accessec GmbH**
Serge van Nuijs, **Adjura**
Chris Payne, **Advanced Cyber Solutions**
Rama Ramachandran, **AGEM jewels**
Filip Lampaert, **BAE Systems AI NV**
and **BAE Systems Applied Intelligence**
David Babin, **Case.one**
Bruno Kerouanton, **CISO Confidential**
Nandakumar Ramakrishnan, **Colruyt Group**
Michel Luypaert, **Confidential**
Gert Maton, **Cranium**
Rachel Hatfield, **Cyber Management Alliance**
Chris Morris, **Cyber Management Alliance**
Allie Philpin, **Cyber Management Alliance**
Amar Singh, **Cyber Management Alliance**
Bal Rai, **Cyber Management Alliance**
Serge Moreno, **Delaware**
Abhijeet Pathania, **Deloitte**
Bernard Grymonpon, **Deltus**
Peter Wright, **DigitalLawUK Ltd**
Rasa Juzenaite, **Dimov Internet Law Consulting**
Rob Demain, **E2E Assure**
Stewart Benger, **E2E Assure**
James Fox, **E2E Assure**
Yves Vandermeer, **ECTEG (European Cybercrime Training and Education Group)**
Delphine Harou, **EDPS**
Touria Akel, **emea-pmo**
Veronique Cimina, **European Institution**
Fabrice Hecquet, **Excellium Services**
Juho Rikala, **Fazer Group**
Ken Nichols, **gdpr-musings.com**
Ken Douglas, **GRC ISMS**
Barry Seward, **GRC ISMS**
Viktoria Mfaume, **I-DATA CONSULT**
Guno Pocorni, **IAP**
Apostolos Tounas, **ING**
Peter Houtmeyers, **ING Belgium**
Kristof Panis, **INGENIUS Law Firm**
Hilde Rietveld, **Ipswitch**
Vladimir Jirasek, **Jirasek Security**
Bob Mann, **Jirasek Security**
Lee Reynolds, **NETconsent**
Dom Saunders, **NETconsent**
Alexander Screve, **Odyssee**
Lars Veelaert, **On IT-services**
Tomas Sikora, **Police CR**
Petr Peca, **Police CR**
Petr Cvacek, **Police CR**
Laurent Bounameau, **Police Fédérale**
Rula Swordsman, **Privacy Dimensions**
Rowena Fielding, **Protecture Ltd**
Kris Troukens, **Quality Hotel Services**
Patrick Vandenbemd, **Rugby Factory**
Frank Louwers, **Rule 11**
Wesley Veldeman, **SecurIT**
Marcus Burkert, **SecurityOfficer.eu**
Petra Bruetsch, **SecurityOfficer.eu**
Cristi Mihalcea, **Self-employed**
John Popolizio, **Shieldox**
Amit Govrin, **Shieldox**
Nathalie Dewancker, **Smals**
Gregory Steenhout, **SpotIT**
Johan Stronkhorst, **Strong Horse Belgium**
Ramses Gallego, **Symantec**
Giselle Van Tornout, **Tilburg University**
Toon De Doncker, **Tittel-IT**
Robert Kloots, **TrustingtheCloud**
Justine Lozina, **Uptime Group**
Sven Bijvoet, **Venn SA/NV**
Frederic Van Keirsbilck, **Verizon Enterprise Solutions**
Mathieu Gorge, **Vigitrust**
Rowan Fogarty, **Vigitrust**
Spyridon Katsikidis, **Wipro**
Mike Thevissen, **WW**

INTRODUCTION

On 13th November 2017, Cyber Management Alliance assembled together practitioners, and thought leaders in cyber security and data privacy from across Europe at their European inaugural Wisdom of Crowds event at the Pullman Hotel Brussels in Belgium.

Wisdom of Crowds is all about providing guidance and sharing knowledge derived from the collective experience of practitioners – 'the wisdom of many surpasses the knowledge of a single few'.

The event, led by Amar Singh, CEO and founder of Cyber Management Alliance, globally recognised cybersecurity thought leader and sought-after keynote speaker, focused on the forthcoming European GDPR, explored how to enable organisations to become GDPR-ready and comply with the new regulations.

From mind maps that covered the key steps, people and technology needed for a GDPR-ready enterprise, the over 70 experienced practitioners created a series of checklists to ask third parties, guiding controllers and processors in how to manage records.

Some of what the Checklists cover include:

Record Keeping Requirements – including corporate mission and vision, data register, records of external audit findings, risk management methodology, DPIA output, privacy notice, training records and data exposed to third parties.

GDPR Readiness – including training and awareness cover, DSAR readiness, DPO, CISO role and formal risk management.

Cyber Incident Planning & Response Maturity – including BCP readiness, cyber response training, SOC site visit and maturity assessment.

Insurance – liability, direct and indirect cover.

Staff – hiring practices, training metrics, subcontractor hiring policies and management approach.

Technical Competencies – including data encryption practices, data destruction/deletion, access management, data portability and exit strategy, certifications and references.

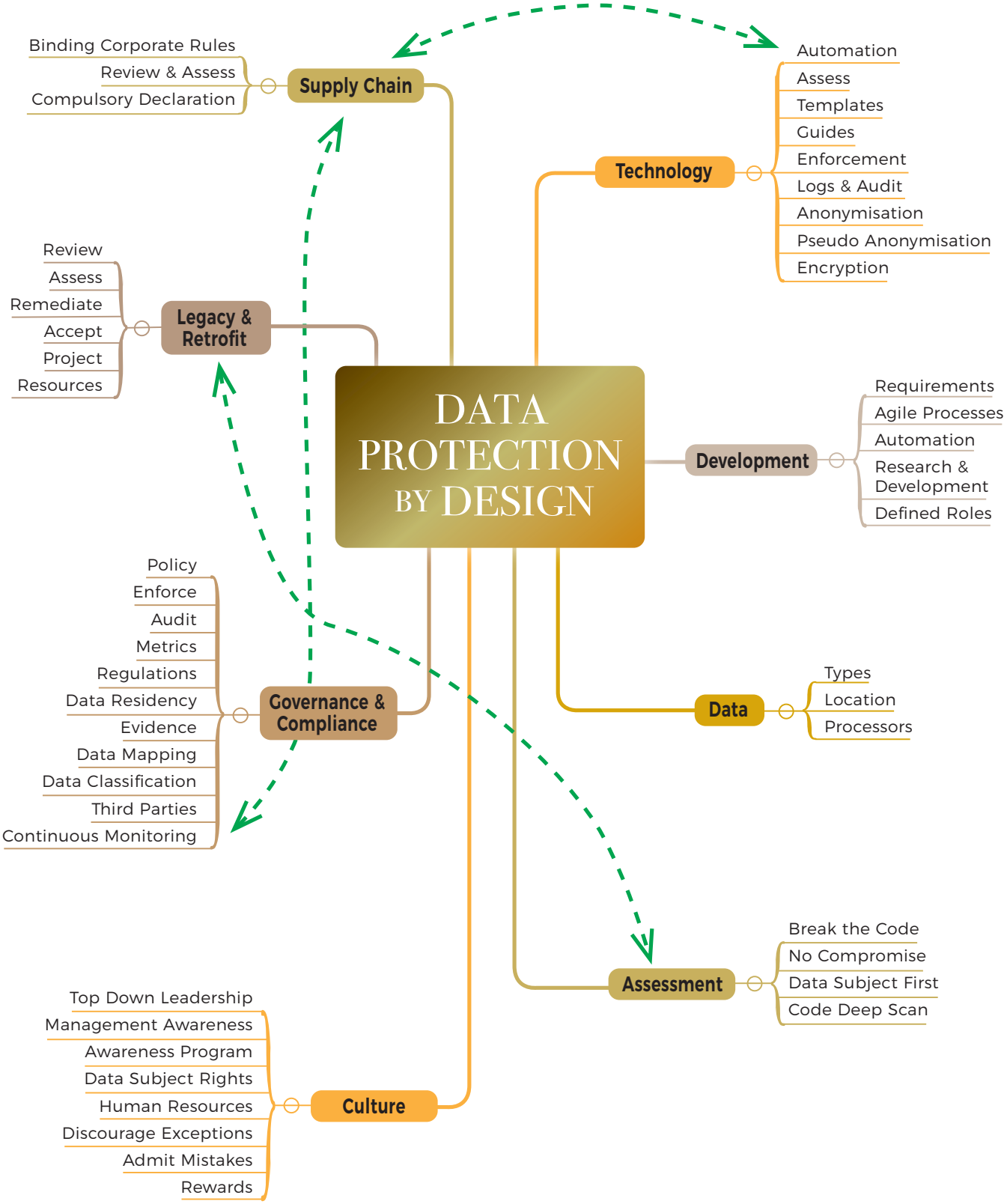
You can follow our unique Wisdom of Crowds 'Data Protection by Design mind map, created by attendees at the Pullman Hotel Brussels event in November. This comprehensive flow chart follows the routes for Supply Chain, Legacy and Retrofit, Technology, Governance and Compliance, Culture, Assessment, Development and Data.

Throughout the European Wisdom of Crowds event, the audience participated in a series of polls around about 'Architecting a GDPR-Ready Enterprise'. The results of the polls provide an informative insight into the minds of GDPR and information security practitioners, and thought leaders.

CHECKLIST TO ASK YOUR THIRD PARTIES & RECORD KEEPING REQUIREMENTS (CONTROLLERS & PROCESSORS)

- **Record Keeping Requirements (Controller & Processor)**
  - Corporate mission & vision
  - Categories of data processed
  - Purpose of processing
  - Data register
  - Data breach register
  - Data sharing register
  - Records of external audit findings
  - Risk management methodology
  - Data processing activities
  - DPIA output
  - High priority incident logs
  - Privacy notice
  - Training records
  - Data exposed to third parties.
- **GDPR Readiness**
  - Overview of current state
  - Training & awareness cover
  - Other audits available for review (ISO 27001)
  - Privacy notice
  - Responsible person / DPO
  - DSAR readiness
  - CISO role
  - Formal risk management
- **Cyber Incident Planning & Response Maturity**
  - Share P1 incidents overview last three years
  - BCP readiness
  - Cyber response training for executives
  - Security Operations Centre (SOC) site visit
  - SOC maturity assessment
- **Insurance**
  - Liability
  - Direct & indirect cover
- **Staff**
  - Hiring practices
  - Training metrics
  - Subcontractor hiring policies
  - Subcontractor management approach
- **Technical Competencies**
  - Data encryption practices
  - Data destruction / deletion
  - Guarantee integrity of the data
  - Access management
    - Role-based access control
    - Audits of access
  - Data
    - Portability
    - Exit strategy
    - Isolation / segregation
    - Deletion
    - Backup
    - Retention
    - Access management
  - Certifications & references
    - Staff skills
    - Accreditations (ISO, SOC, etc)
    - Other government accreditation
    - Customer reference
- **Define roles and responsibilities**
- **Service Level Agreements (SLAs)**

Simplification | Obligation | Privacy | Culture



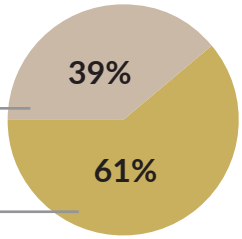
POLL RESULTS

GDPR to my organisation is:

Troublesome compliance requirement: **0%**

An obligation to protect personal information: **39%**

An opportunity to show our competitors, customers and business partners that we have appropriate data protection controls and processes: **61%**



Breach readiness in GDPR starts with:

Having a Cyber Incident Planning & Response strategy..... **25%**

Getting every employee trained on GDPR..... **10%**

Ensuring all senior execs and stakeholders understand the principles of GDPR and breach notification..... **69%**

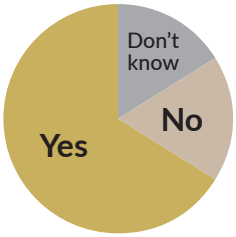
Understanding / mapping all data processing workflows..... **21%**

Do you believe there is a tangible shortage of DPOs?

Yes: **67 %**

No: **18%**

Don't know: **16%**



Is your organisation "ready" for the GDPR?

Yes, bring it on **22%**

Somewhat prepared **53%**

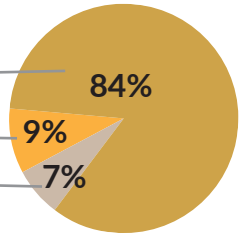
Early stages of research (means no)..... **24%**

Governments must take the lead on GDPR and increase transparency around how and what they do with citizens' data.

Absolutely, agree: **84%**

No, disagree: **9%**

Indifferent, don't care: **7%**



Technology must be used to enforce GDPR principles.:

Yes **62%**

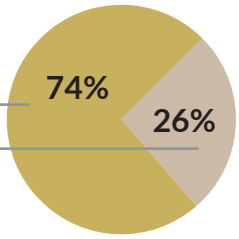
Not Really **38%**

POLL RESULTS

Cookies (most) are a threat to online privacy.

Agree: **74%**

Disagree: **26%**



Governments have done a good job to make businesses aware of the upcoming GPDR regulations.

Yes **11%**

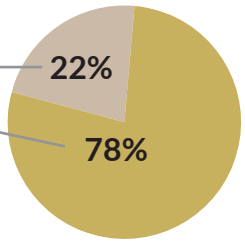
No **74%**

Don't know **15%**

On the topic of Legitimate Interests:

I understand every aspect of this.: **22%**

Need more clarification from regulators: **78%**



Post GDPR - DSAR may be used as a means to launch a DOS attack on a business (think thousands of DSAR per day/week or month):

Yes, worried and prepared..... **12%**

Yes, worried, BUT not prepared..... **64%**

No, not a concern **24%**

In your opinion, in an organisation, which department is most likely to cause a data breach?:

Human Resources (HR): **18%**

Marketing: **61%**

Accounting: **0%**

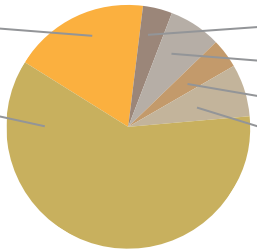
Other: **0%**

4%: Procurement

7%: IT

4%: Legal

7%: Sales



POLL RESULTS

Third parties are a significant risk for potential data breaches (causing a data breach).

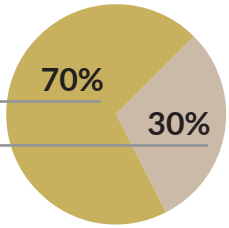
Agree **82%**

Disagree **18%**

In time, consumers/data subjects will judge companies based on their GDPR practices (as in how companies respect and protect personal privacy of customers and employees).

Yes, absolutely: **70%**

Nope, it's a far-fetched idea.: **30%**



Top three challenges in the post GDPR life (say, May 2019 onwards)**:**

Finding and retaining skilled staff. **26%**

Data Management (consent etc)..... **65%**

Managing the underlying security vulnerabilities..... **38%**

Managing and monitoring third party risk and compliance (to GDPR).... **85%**

Being able to swiftly detect and respond to a data breach.. ..... **68%**

In your opinion, what are the TOP three threats that could cause a Data Breach in 2018?:

Ransomware created from recent NSA theft of advanced technologies... **9%**

Mismanagement of privileges and rights within an organisation..... **70%**

Nation state attacks having impacts on organisations (non-Petya).. ..... **9%**

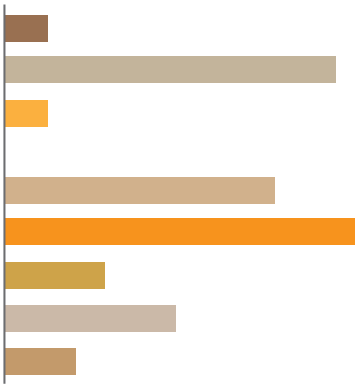
Bad cyber hygiene practices in the cloud and non-cloud data centres – such as misconfiguration, poor vulnerability management..... **57%**

Insufficient training and awareness of employees... ..... **74%**

Poor or non-existent encryption technology.... ..... **21%**

Poorly written and communicated policies..... **36%**

A compliance (tick box) approach to GDPR.... ..... **15%**



POLL RESULTS

One word to describe your experience today at Wisdom of Crowds:

The next Wisdom of Crowds in Brussels must cover:

PLATINUM SPONSOR

e2e assure

We provide cyber security as a service delivered from the cloud to secure your organisation and keep it secure.

We constantly monitor and test your organisation to detect cyber threats, investigate, contain and eradicate them.

We supply cyber services to UK Central Government and Defence.

Where do I start?

Come and talk to us about our free no obligation security advisory service.

If you want more information email us at **info@e2e-assure.com** or visit our website **www.e2e-assure.com**

AT-A-GLANCE

We offer a complete protective monitoring and SOC cyber defence service.

- Provides continuous security monitoring and active incident response
- Defend your business and important data
- Service can be scaled-up or down as the threat landscape changes
- Provides the managed security you need to successfully protect your critical assets from cyber-attacks and data breaches.

The service transforms your organisation's security posture, making it an extremely hard target, proving to your board and customers that you take cyber security seriously.

Objective advisors for the design and supply of efficient and effective IT security solutions

Extensive technical experience from years of design, implementation and support roles.

In depth knowledge of:

- Industry Standards
- Data Protection Legislation
- Compliance Standards

info@advancedcyber.co.uk
www.advancedcyber.co.uk
+44 20 3290 3417

advanced cyber solutions

SILVER SPONSORS

Jirasek security

Information security protection for enterprises

- www.jiraseksecurity.com
- Contact@jiraseksecurity.com
- +44 20 7183 9858

HumanFirewall.io™
EMPLOYEE POWERED INFOMATION SECURITY

Inbound and outbound phishing protection

- http://humanfirewall.io
- info@advancedcyber.co.uk
- +44 20 3290 3417

SHIELDOX

Autonomous PDP FOR DOCUMENTS IN MOTION

- www.shieldox.com
- info@advancedcyber.co.uk
- +44 20 3290 3417

netconsent
Automating Compliance

A leading vendor of compliance and communications software

- www.NETconsent.com
- info@advancedcyber.co.uk
- +44 20 3290 3417

VIGITRUST

VigiTrust is an award winning provider of SaaS based GRC solutions

- www.vigitrust.com
- info@vigitrust.com
- +353 1 453 9143

GRC-ISMS plus

The GRC-ISMS platform is designed to help GDPR compliance

- info@advancedcyber.co.uk
- +44 20 3290 3417

WISDOM OF CROWDS

FOR FURTHER INFORMATION

Please contact
info@cm-alliance.com for more information.

EVENT SPONSORS

Platinum Sponsor

e2e assure

Gold Sponsor

advanced cyber solutions

Silver Sponsors

Jirasek security · SHIELDOX · VIGITRUST · HumanFirewall.io™ EMPLOYEE POWERED INFOMATION SECURITY · netconsent Automating Compliance · GRC-ISMS plus

CYBER MANAGEMENT ALLIANCE

wisdomofcrowds.events