# GDPR

9 Months On

07 February 2019

Ian Fish – Chair of BCS ISSG

# ZDNET – 05/02/2019


Image: European Commission

- EU warns that ENOX Safe-KID-One smartwatches contain several security flaws that let third-parties track and call children's watches.

# ACCENTURE TECHNOLOGY VISION 2019

- **The Next Era of Innovation Will Emphasize Privacy and Individualization**
- Over the next three years, companies will give consumers more control over their data, privacy, and how they interact with products and services.
- "Companies are amassing tremendous amounts of information about consumers," said Paul Daugherty, Accenture's chief technology and innovation officer. "The key thing for companies to think about is just because you can do something doesn't
- Successful brands will have to build trusted relationships with consumers, the report says, and that includes providing transparency and giving consumers control of their data. If consumers trust a brand, they're more likely to offer up even more data in exchange for a better experience—thus continuing the cycle of improving the product or service and growing the business.mean you should do something."

# THE PENALTIES

- 20M Euros or 4% of global turnover whichever is the larger

# HOWEVER

From the ICO Blog

"But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm.

The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick."

# WHAT DOES ALL THIS MEAN


It's a risk thing

# SOME RISKS

- ***Reputational***
- Brand damage
- Loss of client trust
- Loss of employee trust
- ***Operational***
- Individuals' right to stop processing of their data, request correction, deletion or transfer
- Restricted operations
- Data breach

- ***Financial***
- Fines up to 4% and / or 2% global annual turnover
- Litigation costs
- Remediation costs
- ***Regulatory***
- Regulator right to conduct audits, and obtain access to premises
- Imposed limitations
- Rectification costs

# PRINCIPLES

- Under the GDPR, the data protection principles set out the main responsibilities for organisations.

# SCOPE

**In Scope**

- Automated (electronic) *and* Manual (paper) processing of personal data
  - NB: CCTV is also personal data

- Location
- GDPR applies if the following is in the EU:
  - the organisation processing the data; or
  - the data subject; or
  - the processing itself

**Out of Scope**

- Household activity: data processed by an individual for purely personal reasons or for activities carried out in one's home (provided there is no connection to a professional or commercial activity)
- Processing of personal data of deceased persons or of legal entities
- Law enforcement, national security, public security, immigration

# MAJOR CHANGES

# LEGAL BASIS

- Consent
- Contract
- Controller's legal obligation
- Protection of vital interests of subject or other natural person
- Public interest or vested authority
- Legitimate interest

# AND ALSO

- Processor liabilities
  - GDPR directly regulates data processors for the first time.
    - Maintain adequate documentation (Article 30)
    - Implement appropriate security standards (Article 32)
    - Carry out routine data protection impact assessments (Article 32)
    - Appoint a data protection officer (Article 37)
    - Comply with rules on international data transfers (Chapter V)
    - Cooperate with national supervisory authorities (Article 31).
  - Controllers must ensure that there is a written data processing agreement in place with their processors meeting the requirements of GDPR (Article 28)
  - Processors will be directly liable to sanctions (Article 83) if they fail to meet these criteria and may also face private claims by individuals for compensation (Article 79).

# INDIVIDUAL RIGHTS

Right to be informed
Right of access
Right to rectification
Right to erasure
Right to restrict processing
Right to data portability
Right to object
Rights related to automated decision making including profiling

# REGULATORY GUIDANCE?

- ICO – ico.org.uk
  - Guide to the GDPR – now linked to EDPB (formerly Article 29 Working Party) guidance
  - All aspects covered.
  - Also now links to DPA 2018 and LED.
  - ICO Blogs

# REGULATORY GUIDANCE?

- EDPB (Article 29 Working Party)
  - Individuals' rights
    - Data portability
    - Personal data breach notification
    - Consent
    - Transparency
  - Controllers and Processors
    - Data Protection Officer
    - DPIAs for high risk processing
    - Personal data breach notifications
    - Automated decision making and profiling
    - Lead supervisory authority

# CONTRACTS

- What do you need to do?
  - Due Diligence
  - Prolonged negotiations
  - Concerns about risk
  - Uncertainty about documenting responsibilities
  - Lack of clarity on GDPR strategy
  - Liability concerns
  - Article 82 and liability claims
  - Indemnification
  - Mutual protections
  - Pushback on subcontracting, security and audit
  - Volume: Existing Contracts

# PROFILING AND AUTOMATED DECISION MAKING

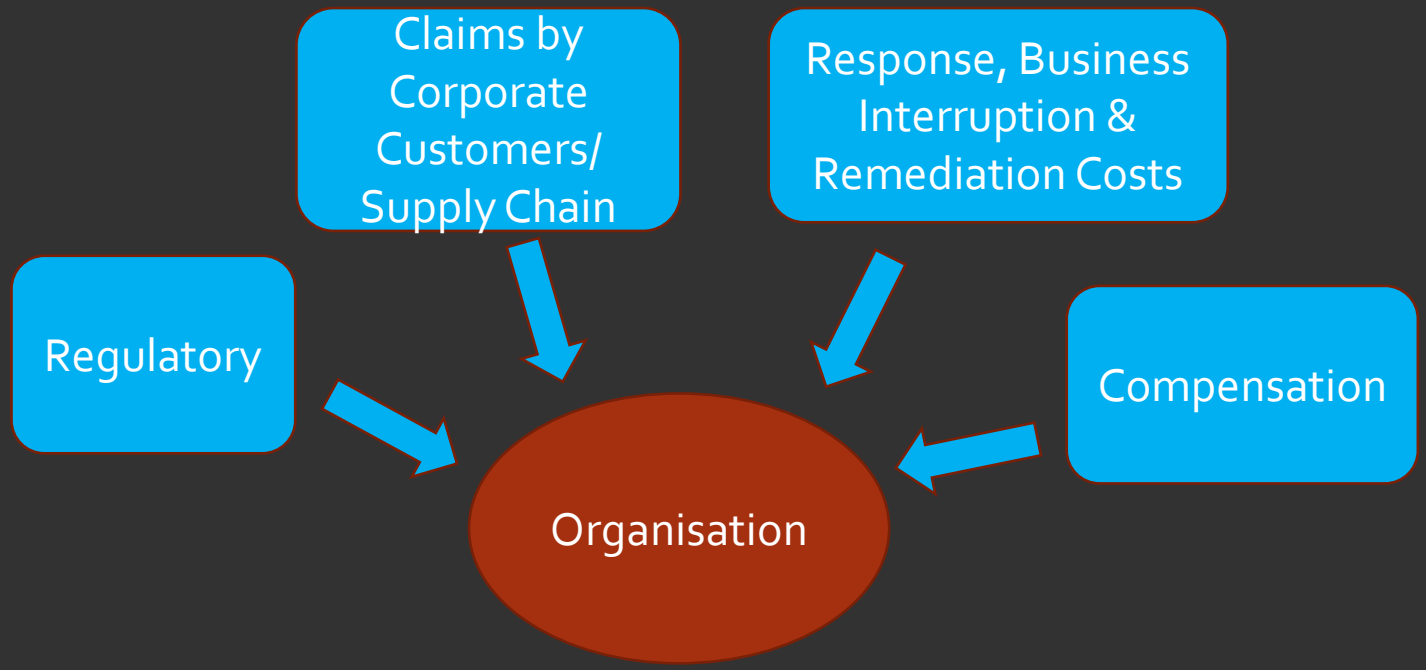
- Expansive guidance now available
- Profiling v Automated Decision Making
- Based solely on automated decision making
- "legal effect or similarly significantly effects"
- Application of Article 22 and consent
- Right not to be subject to decision
- Right of access
- Right to be informed

# BREACH REPORTING

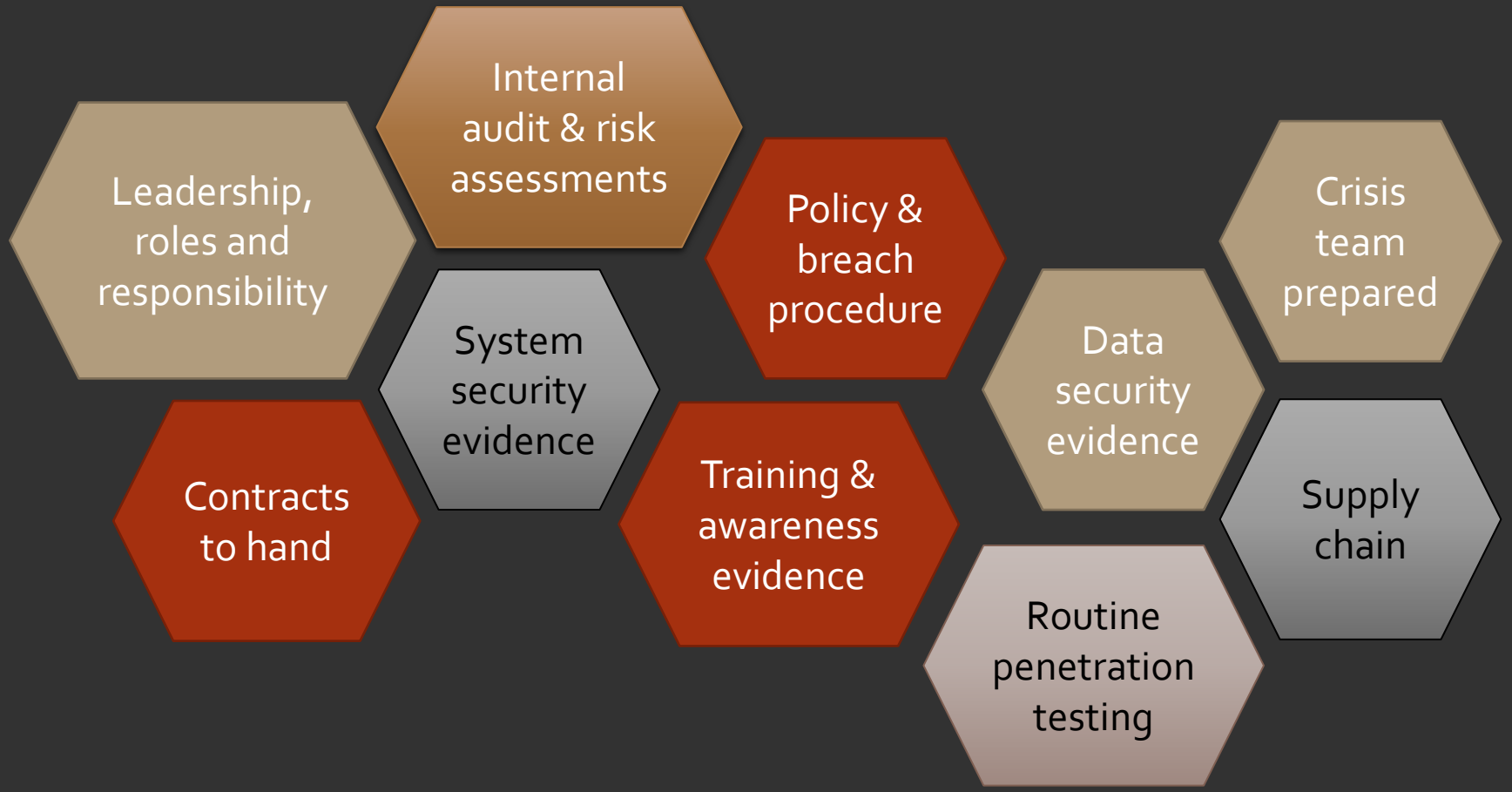
- A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

- You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.
- A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.

# BREACHES – RISKS FROM MANY DIRECTIONS



# IF YOU WERE BEING AUDITED BY ICO



# WHY A UK BILL/ACT

- The EU data protection reform package is not limited to the GDPR; the Law Enforcement Directive must also be implemented by Member States;
- The GDPR only applies to a limited set of activities i.e. those areas of activity within EU competence, so Member States have to address those areas outside EU competence, including national security;
- The GDPR leaves a number of areas for Member States to determine, in particular exemptions and additional grounds for processing personal data in the special categories.

# WHAT DOES IT COVER

- Legislates for:
  - derogations from the GDPR;
  - grounds for processing special category personal data and criminal data;
  - the establishment and powers of the ICO;
  - A number of new, specific national provisions.
- Implements the Law Enforcement Directive;
- Establishes a new DP regime for the national security agencies; and
- Extends the GDPR to those areas outside EU competence not otherwise covered by the other regimes "the applied GDPR".

# STRUCTURE

ICO establishment and powers apply to all areas

The same grounds for processing and derogations apply to GDPR and applied GDPR

Law Enforcement regime

GDPR

Applied GDPR

National Security regime

# DPA 2018 OVERVIEW – GROUNDS FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA

- Personal data about criminal convictions etc.. (Article 10) are generally treated in the same manner as special category personal data;
- The provisions generally reproduce the grounds for processing sensitive personal data under the DPA 98;
- The new grounds for processing special category personal data include journalism in connection with unlawful acts and dishonesty, suspicion of terrorist financing or money laundering, third party processing for group insurance policies and anti-doping in sport.

# ADDITIONAL SAFEGUARDS

- Some of the grounds are slightly wider than the current law e.g
  - Health and social care includes occupational medicine
  - Wider categories of personal data can be processed for equality of opportunity.
- Some types of processing special category personal data require additional safeguards: e.g.
  - Research purposes
  - Employment, social security and social protection law

# DEROGATIONS - OVERVIEW

- Main intention of UK Bill is to preserve and reapply exemptions under Data Protection Act 1998 to the GDPR and "applied GDPR"
- Separate exemptions for law enforcement and national security services
- Existing exemptions for journalistic, literary, archiving etc. purposes maintained
- Five broad classes of exemption

# CLASS 1 EXEMPTIONS

**Scope of exemptions**

- Information requirements under Arts. 13-14
- Data subject access (Art. 15)
- Rectification (Art. 16)
- Erasure (Art. 17)
- Restriction of processing (Art. 18)
- Data portability (Art. 20)
- Objection (Art. 21)
- Article 5(1)(a-b) in respect of lawful processing, and other principles under Art. 5 so far as they relate to rights and obligations relating to above data subject rights

*See Schedule 2, Part 1, para. 1*

**Applies to…**

- crime and taxation
- immigration
- information requiring disclosure under law re legal proceedings
- [protecting effectiveness of armed forces]

# CLASS 2 EXEMPTIONS

## Scope of Exemptions

- **Information requirements under Arts. 13-14**
- **Data subject access (Art. 15)**
- **Rectification (Art. 16)**
- **Erasure (Art. 17)**
- ***See Schedule 2, Part 2, para. 6 and Schedule 3, Part 1, para. 1***
- **Restriction of processing (Art. 18)**
- **Data portability (Art. 20)**
- **Objection (Art. 21)**
- **Principles under Art. 5 so far as they relate to rights and obligations relating to above data subject rights**

## Applies to…

- functions designed to protect the public, etc.
- parliamentary privilege
- crown honours, dignities and appointments
- judicial appointments, judicial independence and judicial proceedings
- health data
- social work data
- education data
- child abuse data

# CLASS 3 EXEMPTIONS

- **Scope of exemptions**
- Information requirements under Arts. 13-14

- *See Schedule 2, Part 4, para. 16*

- **Applies to…**
- legal professional privilege
- corporate finance
- management forecasts and planning
- negotiations

- Data subject access (Art. 15)
- Principles under Art. 5 so far as they relate to rights and obligations relating to data subject access

- confidential references
- exam marks and exam scripts
- self-incrimination

# CLASS 4 EXEMPTIONS

## Scope of exemptions

- Data subject access (Art. 15)
- Principles under Art. 5 so far as they relate to rights and obligations relating to data subject access
- ***See Schedule 4, para. 1***

## Applies to…

- human fertilisation and embryology information
- adoption records and reports
- statements of special educational needs
- parental order records and reports

# CLASS 5 EXEMPTIONS

## Scope of exemptions

- Right of access (Art. 15) and the principles under Article 5 so far as the provisions correspond to the rights and obligations in respect of data subject access
- *See Schedule 2, Part 3, para. 14*

## Applies to…

- situations to the extent that the disclosure of such information would involve disclosing information relating to another person who can be identified from the information

# AUTOMATED DECISION MAKING

- The grounds for processing special category personal data extend the ability of data controllers to make automated decisions;
- Article 22 GDPR permits automated decision making where:
  - The individual has consented
  - It is necessary for a contract or
  - It is authorised by Member State or Union law which also lays down safeguards to protect the data subject's interests
- Clause 13 applied the additional safeguards that data subjects must be notified and able to request a new decisions on a non-automated basis

# POWERS OF ICO AND ADDITIONAL NEW PROVISIONS

- The ICO will be able to charge fees which will be set by the Secretary of State;
- The ICO will be required to establish a number of codes of practice including on data sharing and on direct marketing;
- There are two new criminal offences:
  - Re-identifying information that is de-identified personal data and
  - Taking action aimed at preventing the disclosure of personal data in response to a SAR.

# PSEUDONYMISATION AND ANONYMISATION

- Pseudonymisation is a measure to enhance “appropriate organisational and technical measures” to ensure adequate protection of personal data.
- Anonymisation – as it is dealt with in GDPR – is a chimera.

# BREXIT

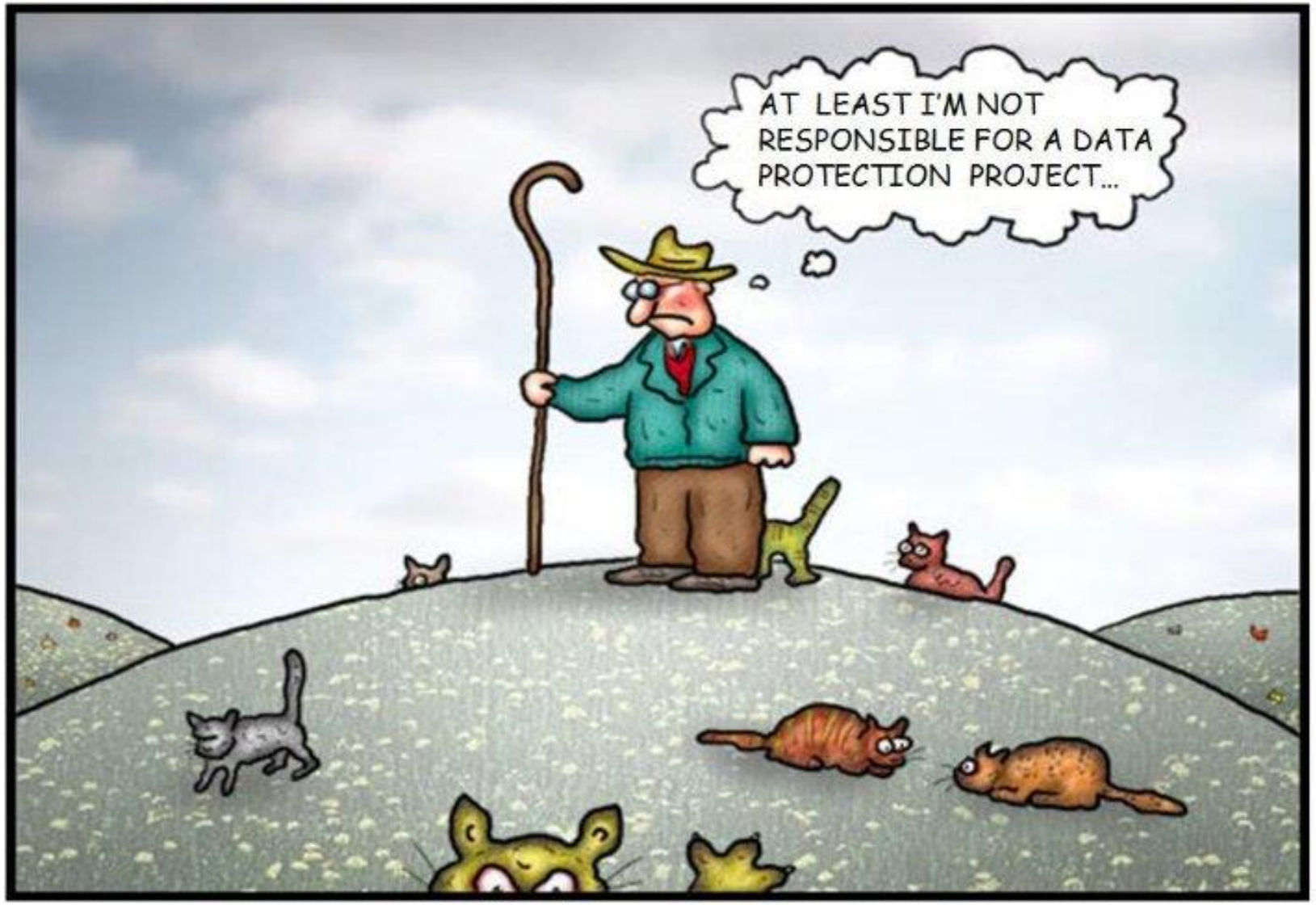
- Adequacy
- Other mechanisms
- The UK's stance

# CDPD (COMPUTERS, PRIVACY AND DATA PROTECTION) CONFERENCE 2019

- Big Topics
  - Access – how good is it?  It is the basis of the rights and freedoms of individuals but the general feeling was that large organisations had processes but were not yet sure how good they are and many SMEs just ignore and hope that they are too small to be bothered with by the SA.
  - Smart Cities and Privacy – all data is personal data; devices are often not patchable/upgradeable; the Toronto experiments (Google as Cyber Labs).
  - Hidden Data Ecosytem – 3 layer model; Data brokers are the problem – one researcher bought dating profiles for 164 persons sorted by religion and sexual preferences for $90.
  - 6 countries in EU have not implemented into national law.
  - Privacy is not the only fundamental right.
  - Facial recognition proliferation and lack of oversight.


TODAY
HAVE YOU BEEN MISSOLD PAYMENT PROTECTION INSURANCE?
GDPR
HAS YOUR PERSONAL DATA BEEN USED WITHOUT THE CORRECT CONSENT, IS IT BEING PROCESSED IN AN UNAUTHORIZED JURISDICTION OUTSIDE THE EU?
FUTURE
©2017 D2LT


"Can someone help me with GDPR?"




The daydreams of cat herders...

# THANK YOU FOR LISTENING


Ian Fish

ANFI Ltd

piscene1@gmail.com

+44 7557 419776