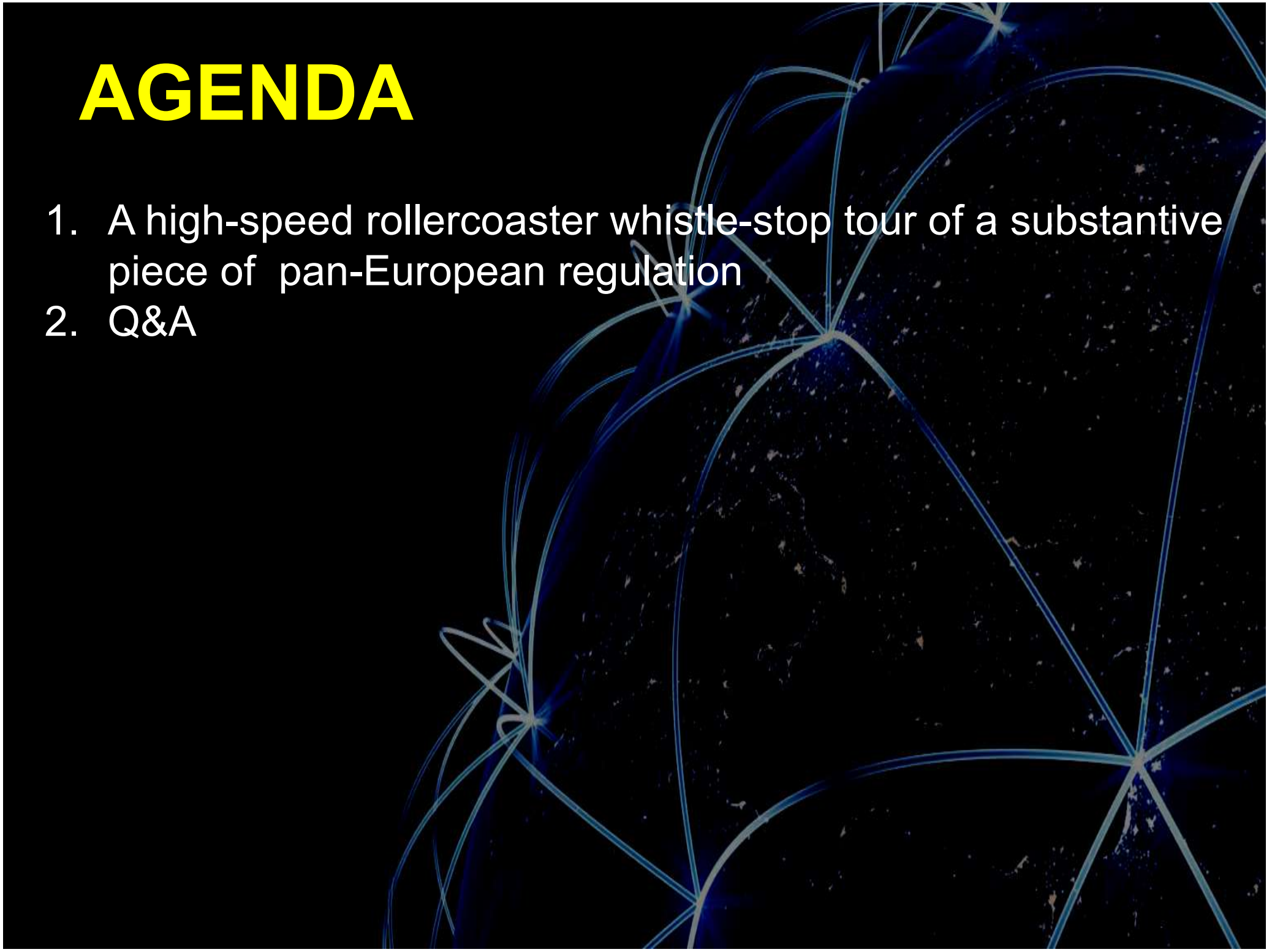
GENERAL DATA PROTECTION REGULATION FOR THE IRISH WASTE MANAGEMENT INDUSTRY

Valerie Lyons – BH Consulting

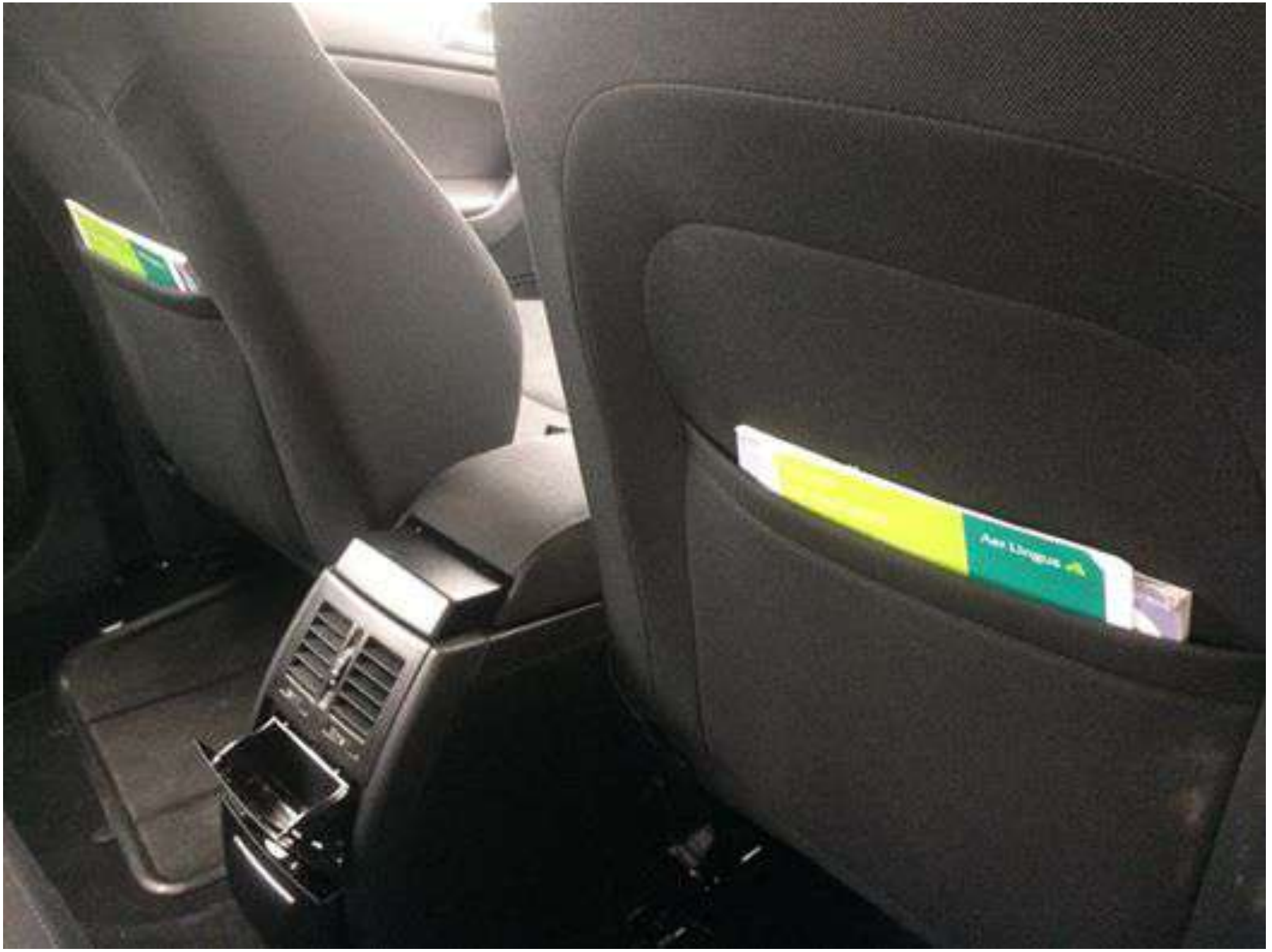
AGENDA

1. A high-speed rollercoaster whistle-stop tour of a substantive piece of pan-European regulation
2. Q&A



Who is Valerie Lyons?

- Ex CISO – KBC (15yrs)
- Started my career in IBM, almost 30 years ago.
- Honorary Fellow of the IISF since 2003
- COO of BH Consulting, and PhD Scholar
- Master in Business & Leadership and degree in Information Systems
- As passionate about Information Privacy and Protection as her son is about airplanes……



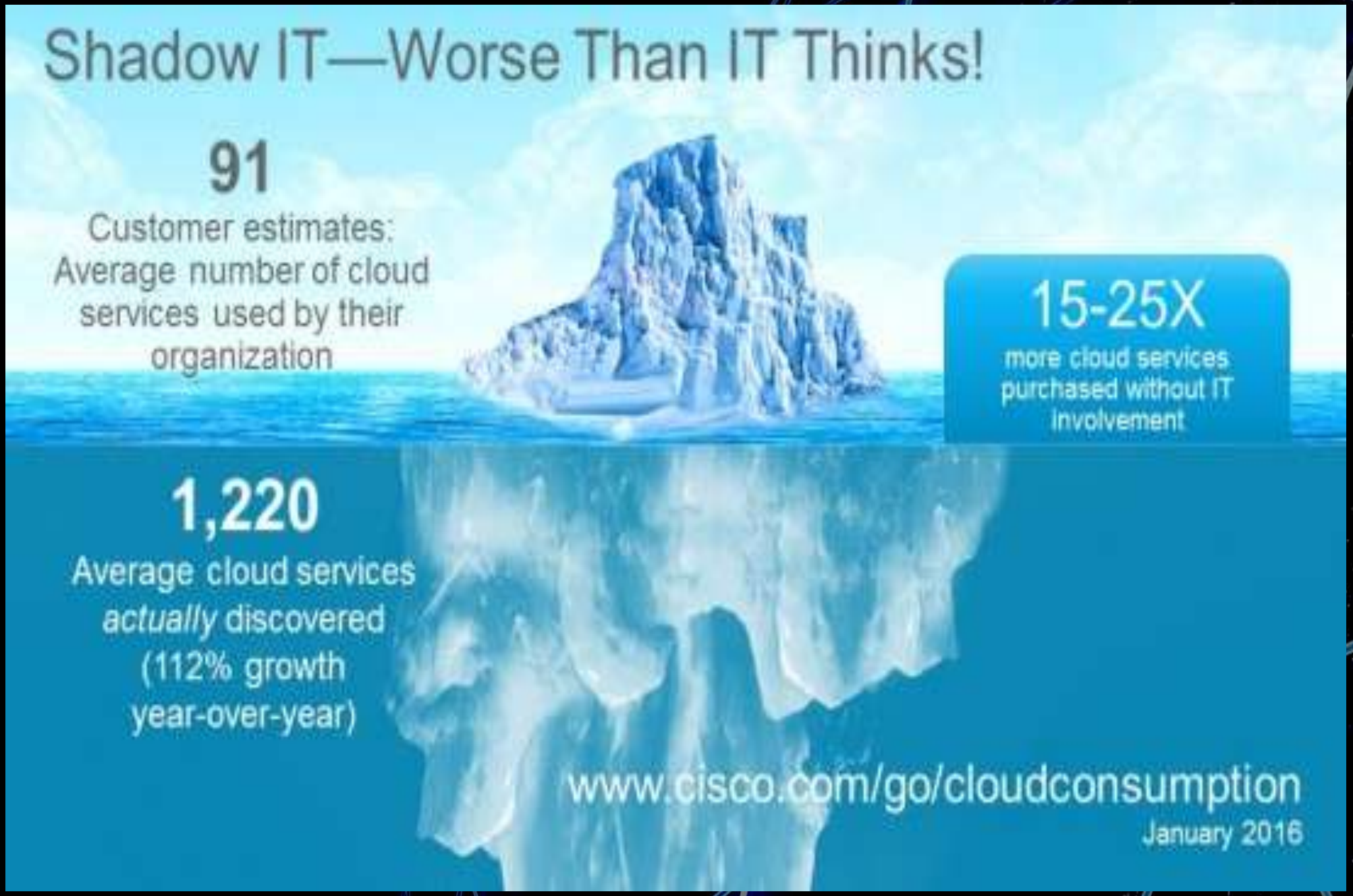
Approaches to protect data?

- Government Regulation
- Industry Self-Regulation
- Data Protection Technologies
- Individuals (Consumers AND Employees) – choices and behaviours, understanding and awareness.

Regulatory Headaches….

- **GDPR (Due 2018)**
- **HIPAA**
- Child Protection Law
- **Privacy Shield (Safe Harbor)**
- Digital Information Act 2017
- Freedom of Information Act
- **Consumer Protection Codes**
- **PCI DSS(Credit Cards)**
- ……etc.

“Are you really compliant….”



GDPR!!

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties: fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as

genetic | mental | cultural | economic | social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Yes

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data controllers must ensure adequate contracts are in place to **govern data processors**.

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

Controllers must have a **legal basis for processing** and collecting personal data.

One-stop shop: international companies will only have to deal with one supervisory data protection authority.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

You have to comply with EU GDPR by MAY 2018

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties:
fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as

genetic

mental

cultural

economic

social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data controllers must ensure adequate contracts are in place to **govern data processors**.

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

Controllers must have a **legal basis for processing** and collecting personal data.

One-stop shop: international companies will only have to deal with one supervisory data protection authority.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

You have to comply with EU GDPR by MAY 2018

What is personal data?

- Name
- Address
- Localisation
- Online identifier
- Health information
- Income
- Cultural profile
- and more

COLLECT
STORE
USE
DATA?

You have to abide by the rules.

What is Sensitive Data

- Racial, Ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sexual orientation

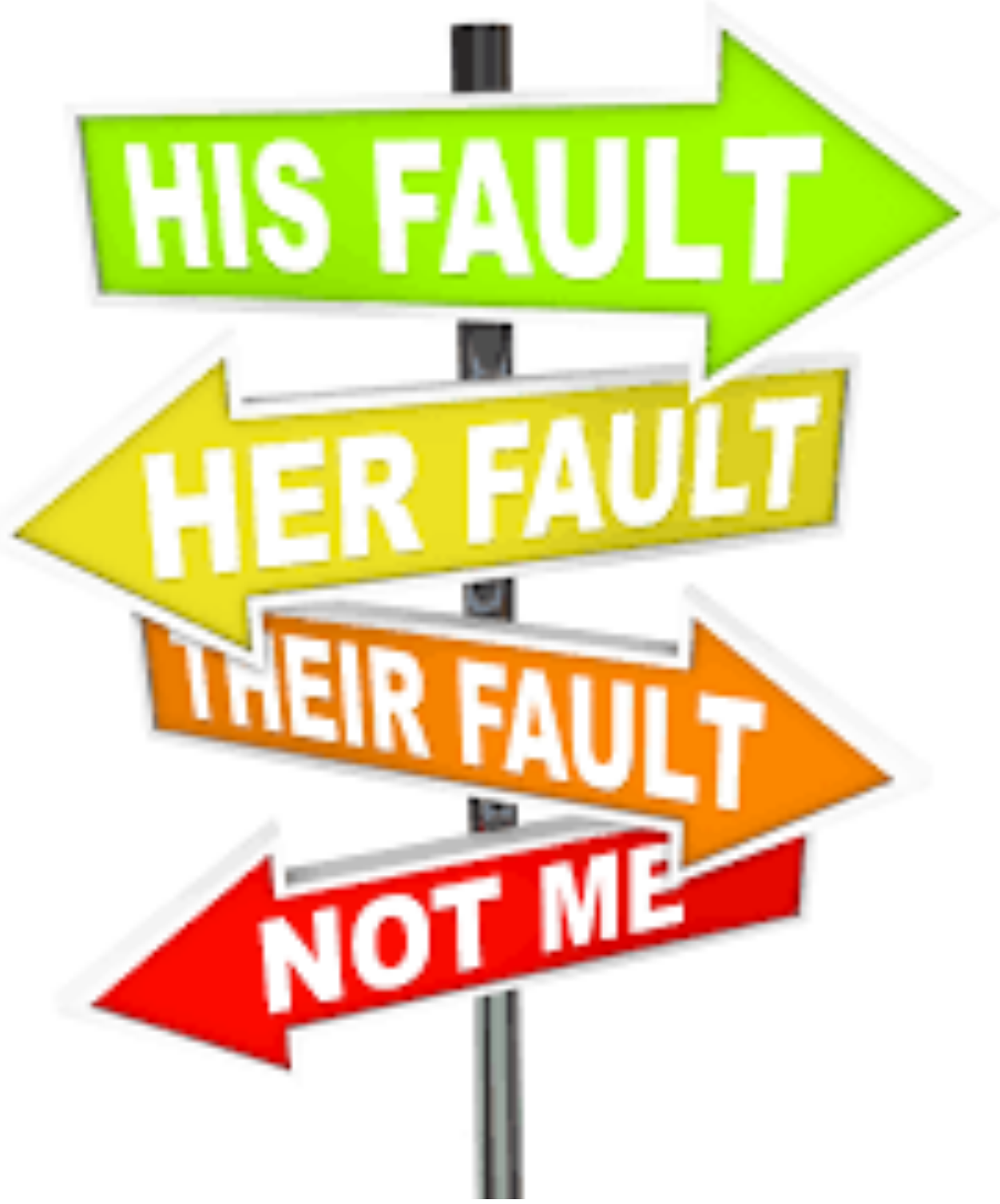
Legal Basis for Processing

At least one lawful basis must apply to process data

1. Legitimate Business Interest
3. Contractual Necessity
4. Compliance with Legal Obligations
5. Consent
6. Vital Interests
7. Public Interest
8. Criminal offences data or civil law enforcement

Data Protection Principles

1. Lawfulness, fairness & transparency
2. Purpose Limitation
3. Integrity & Confidentiality
4. Accuracy
5. Data minimisation
6. Storage limitation
7. Accountability


HIS FAULT
HER FAULT
THEIR FAULT
NOT ME

Principle of Accountability….

- Article 5: *Principles relating to processing of personal data*
- "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). "

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security

Accountability

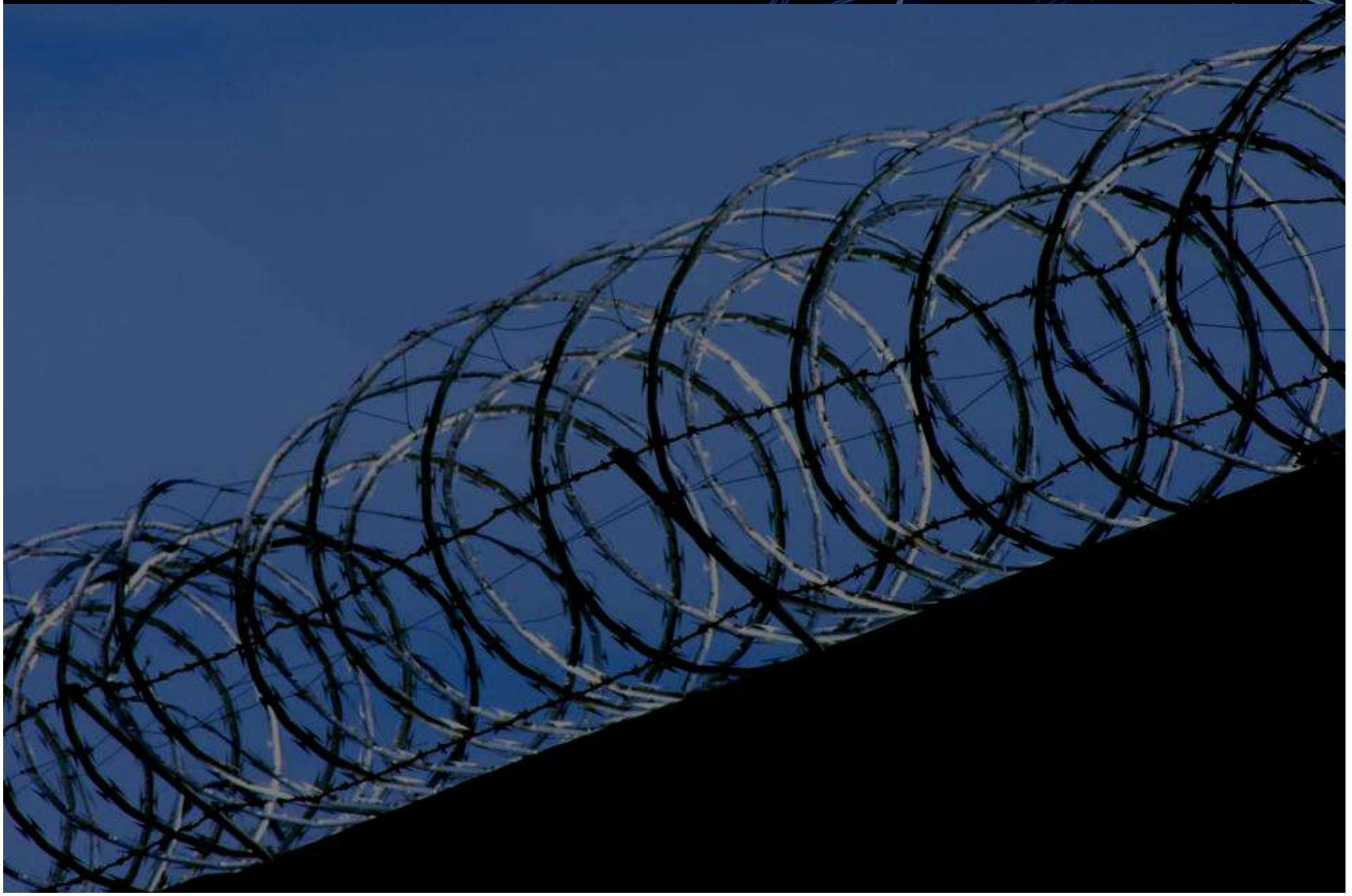
Data Subject Rights

Right of Access
Right to be Forgotten
Right to Object
Right to Profiling Objection (not to be profiled)
Right to Portability
Right to Transparent Communication
Right of Rectification
Right to Restrict Processing

Other Important Aspects

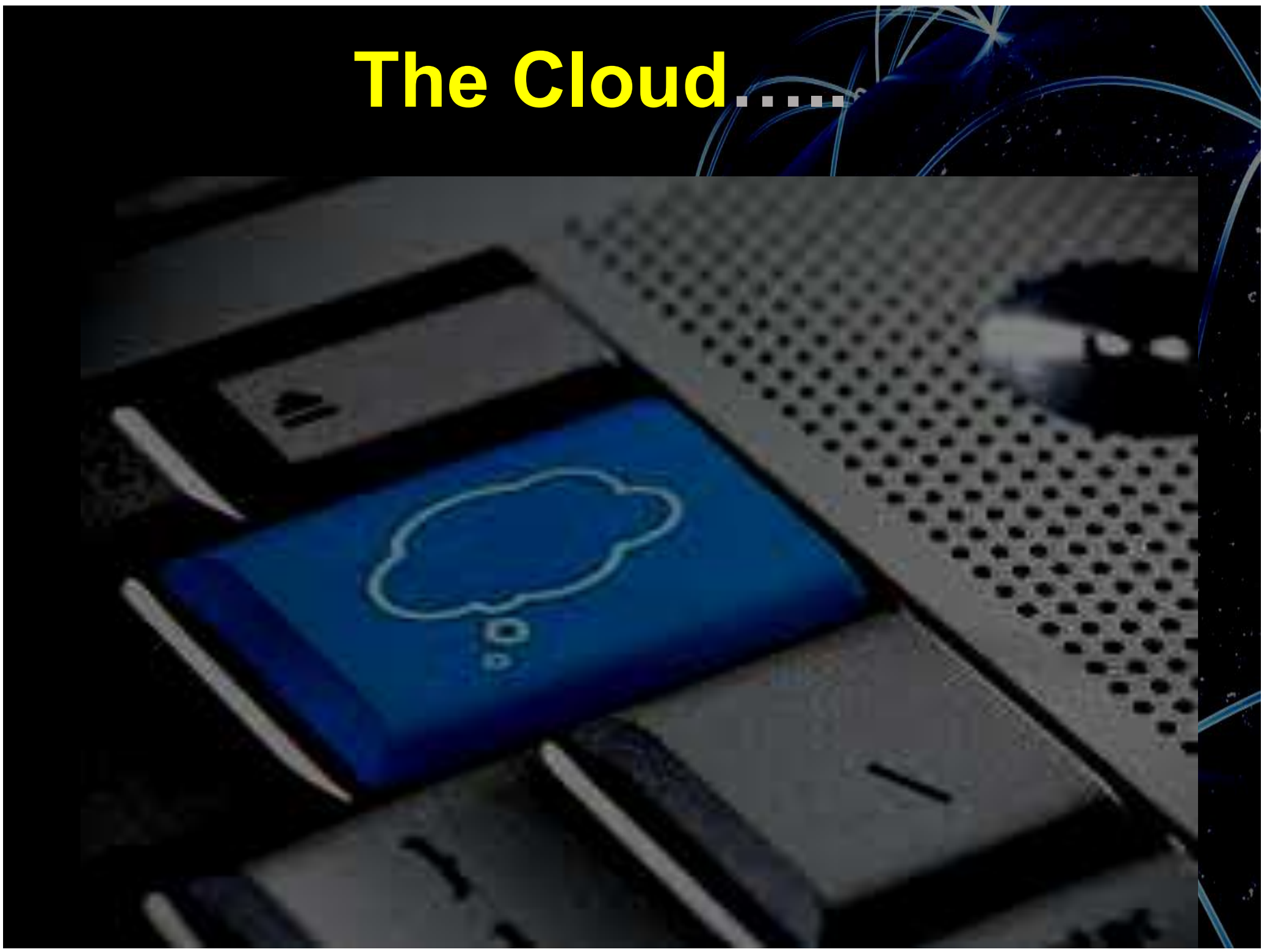
Data Protection Officer…warning!
Data Protection Impact Assessment
Privacy by Design and Privacy by Default
Registration Process
Mandatory Breach Notification
Privacy Policies
Subject Access Requests
Research Exemptions

Data Protection Methods



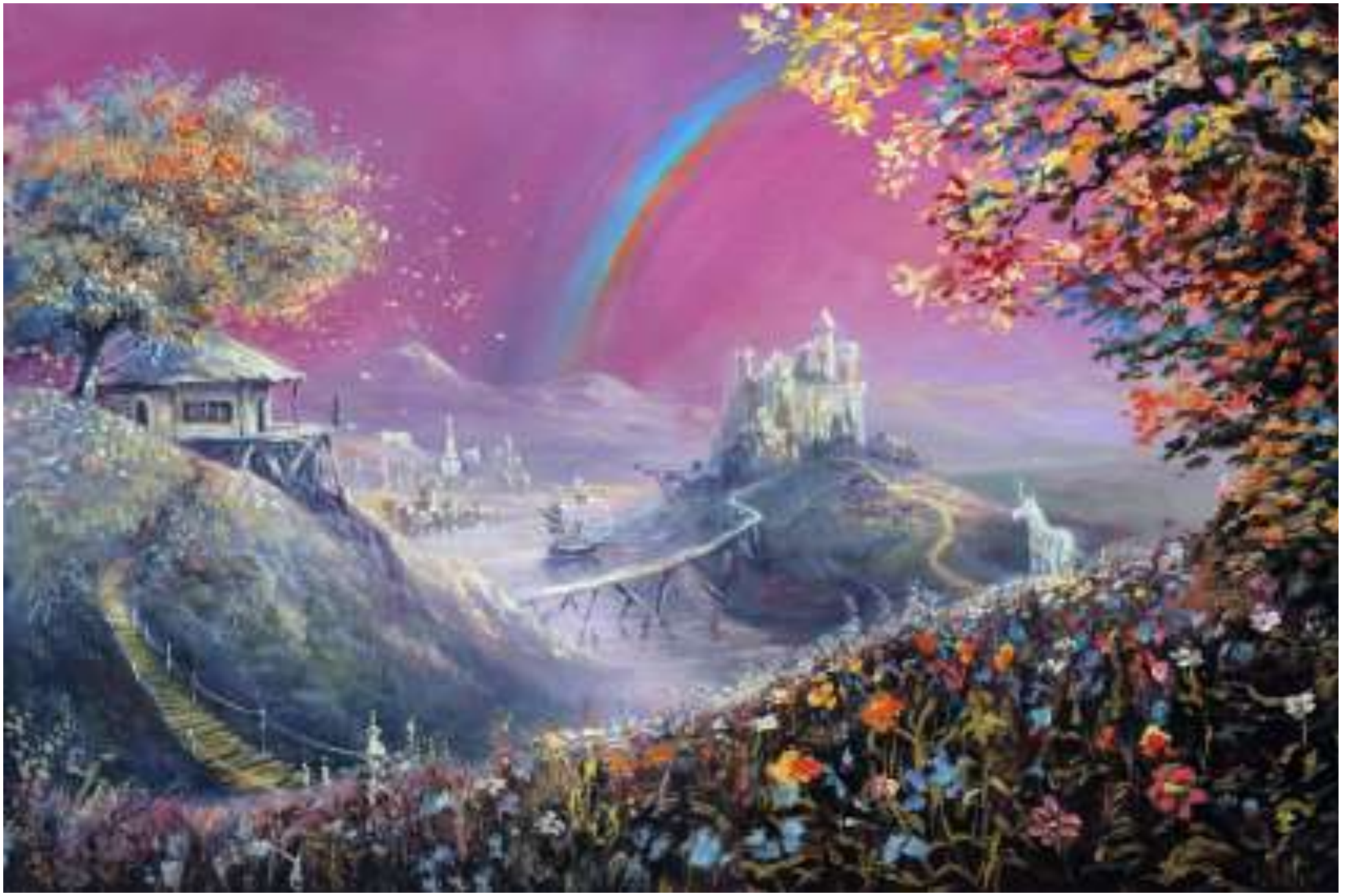
How To Protect Against Data Breaches

The Cloud……

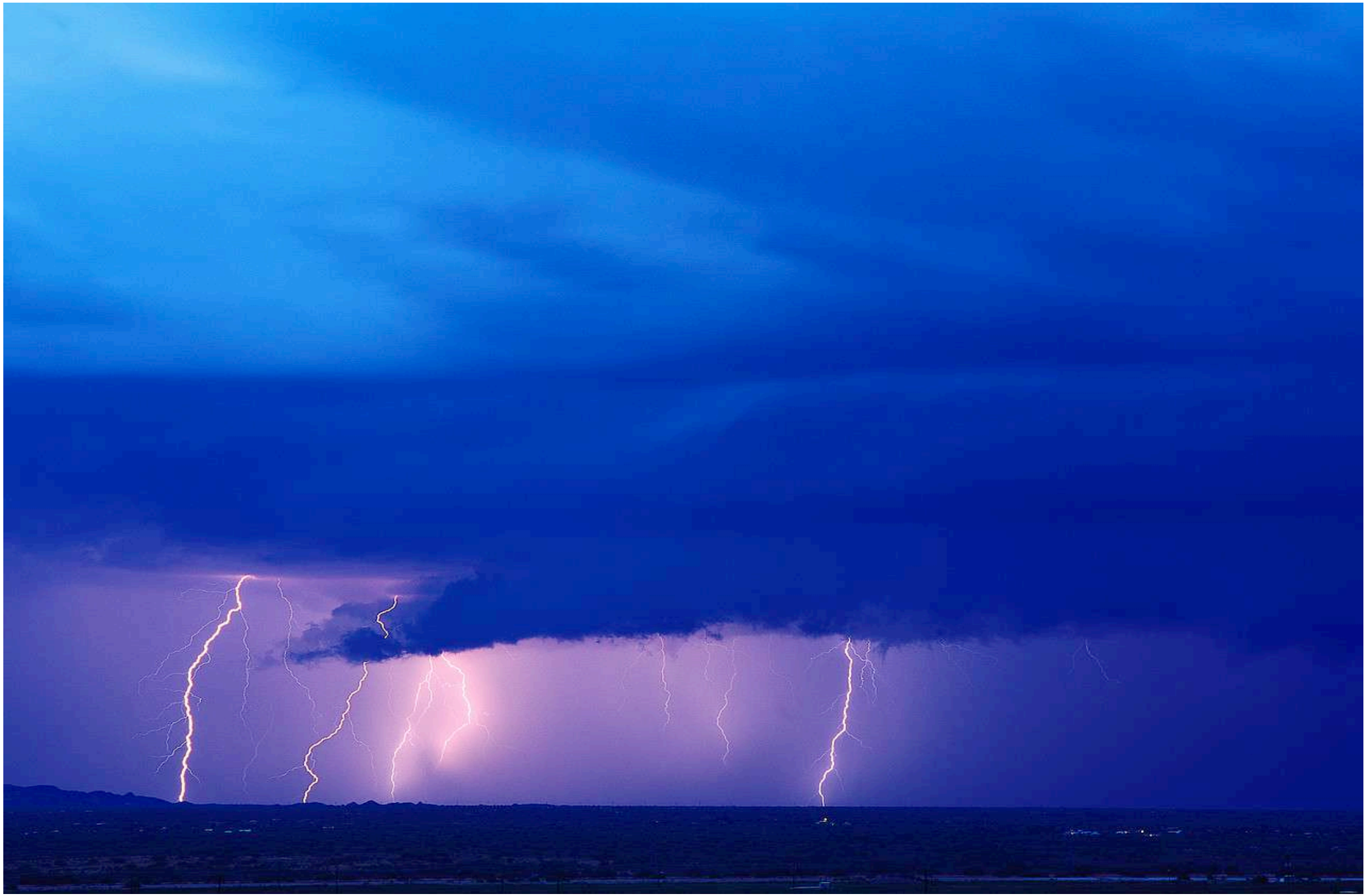


Business View of Cloud Computing

Vendors' View of Cloud Computing

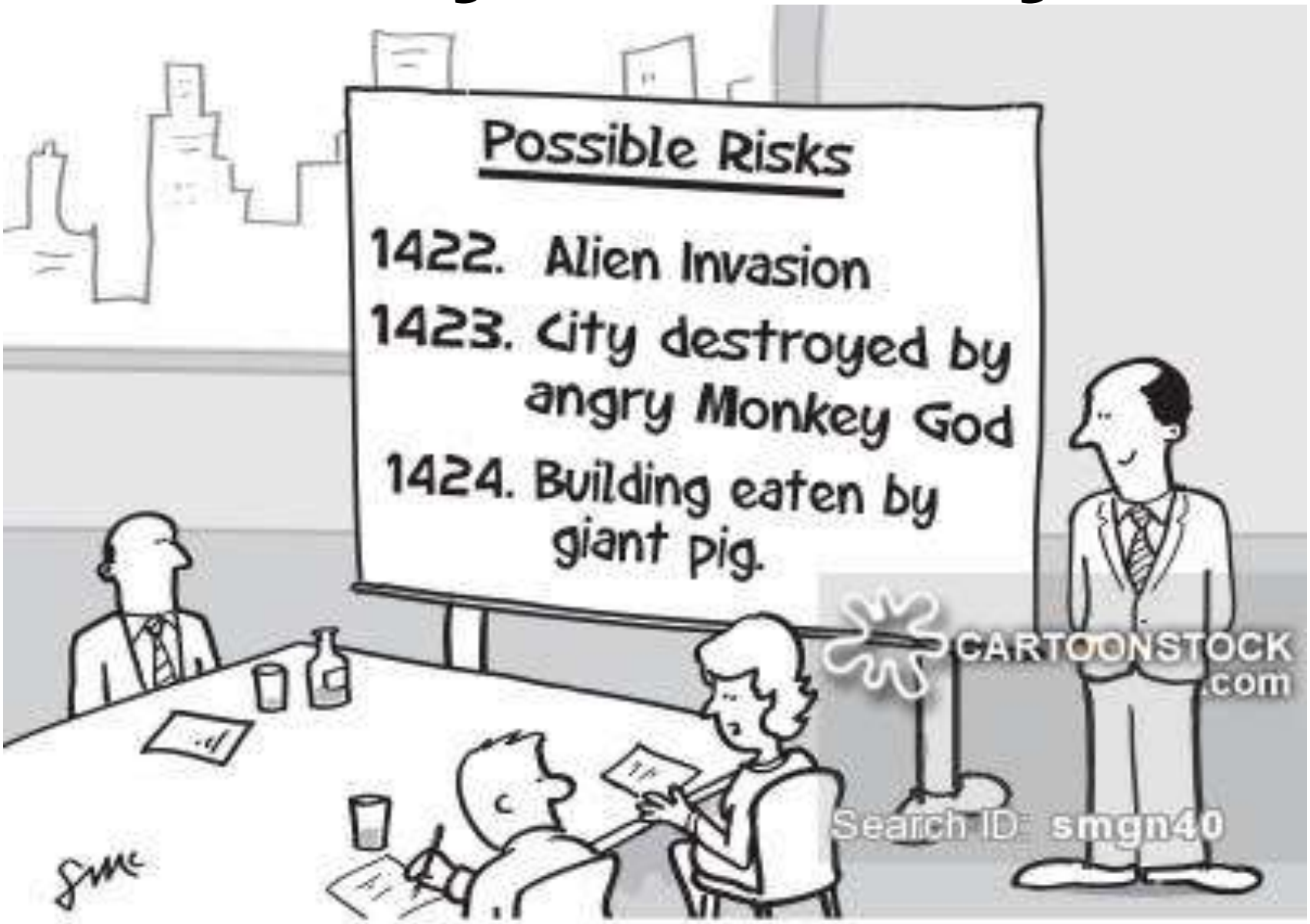


Security View of Cloud Computing



Risk Management Process

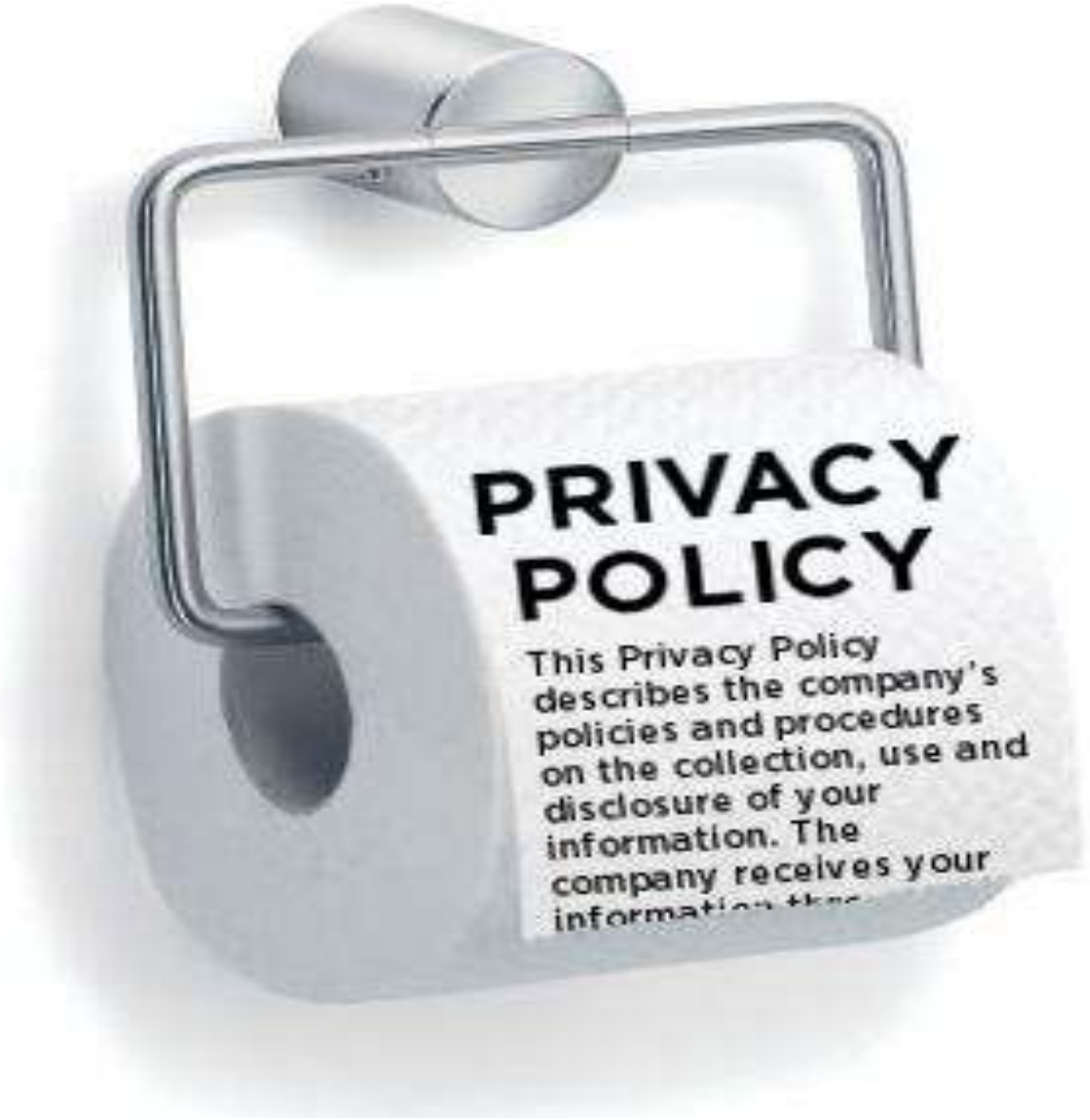
Security Risk Analysis



"Well he certainly does a very thorough risk analysis."

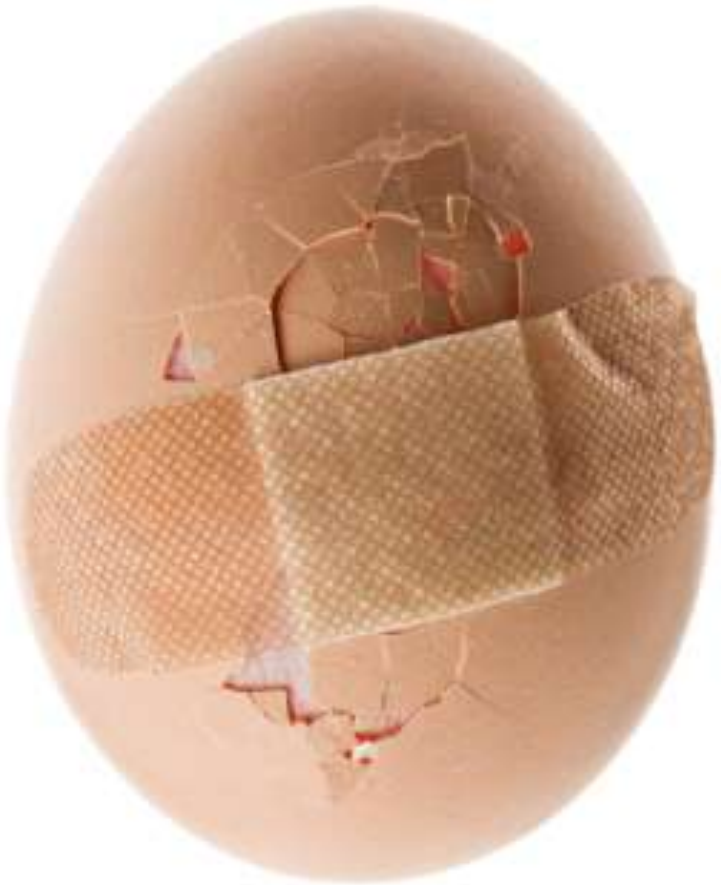
Security Awareness Training

Stakeholder Policies (…T&Cs)

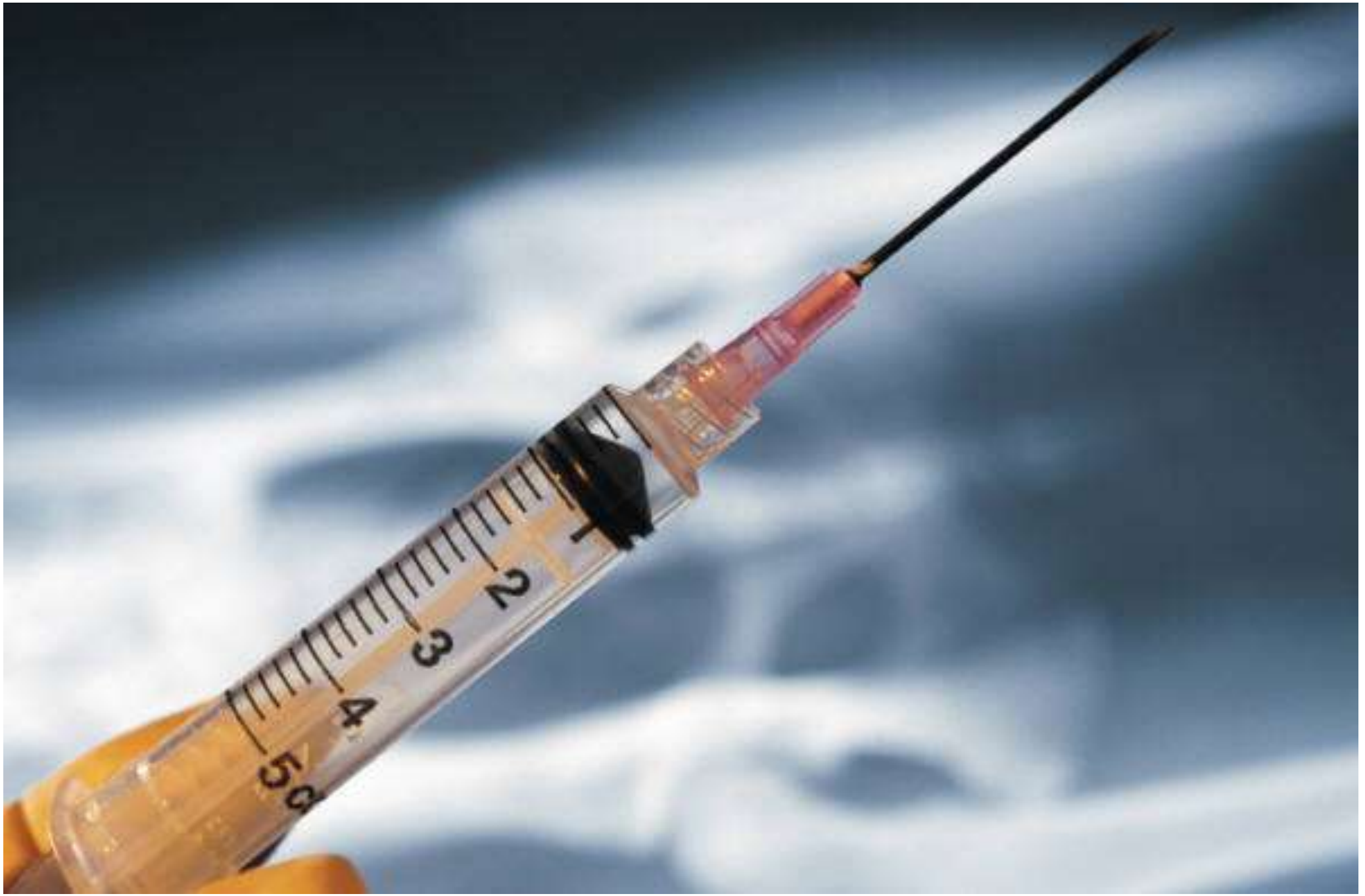


Information Classification

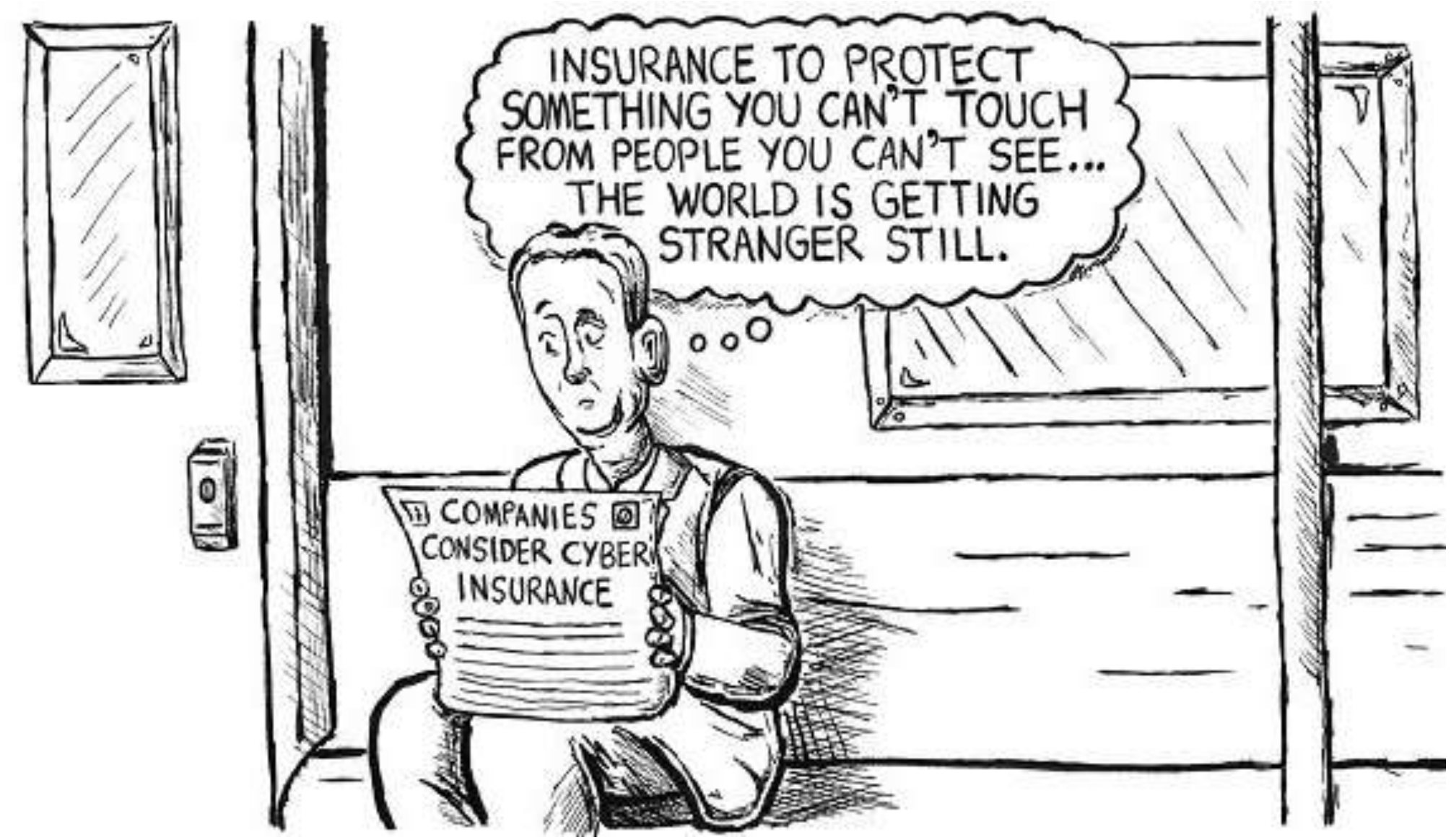
Patching and Updates



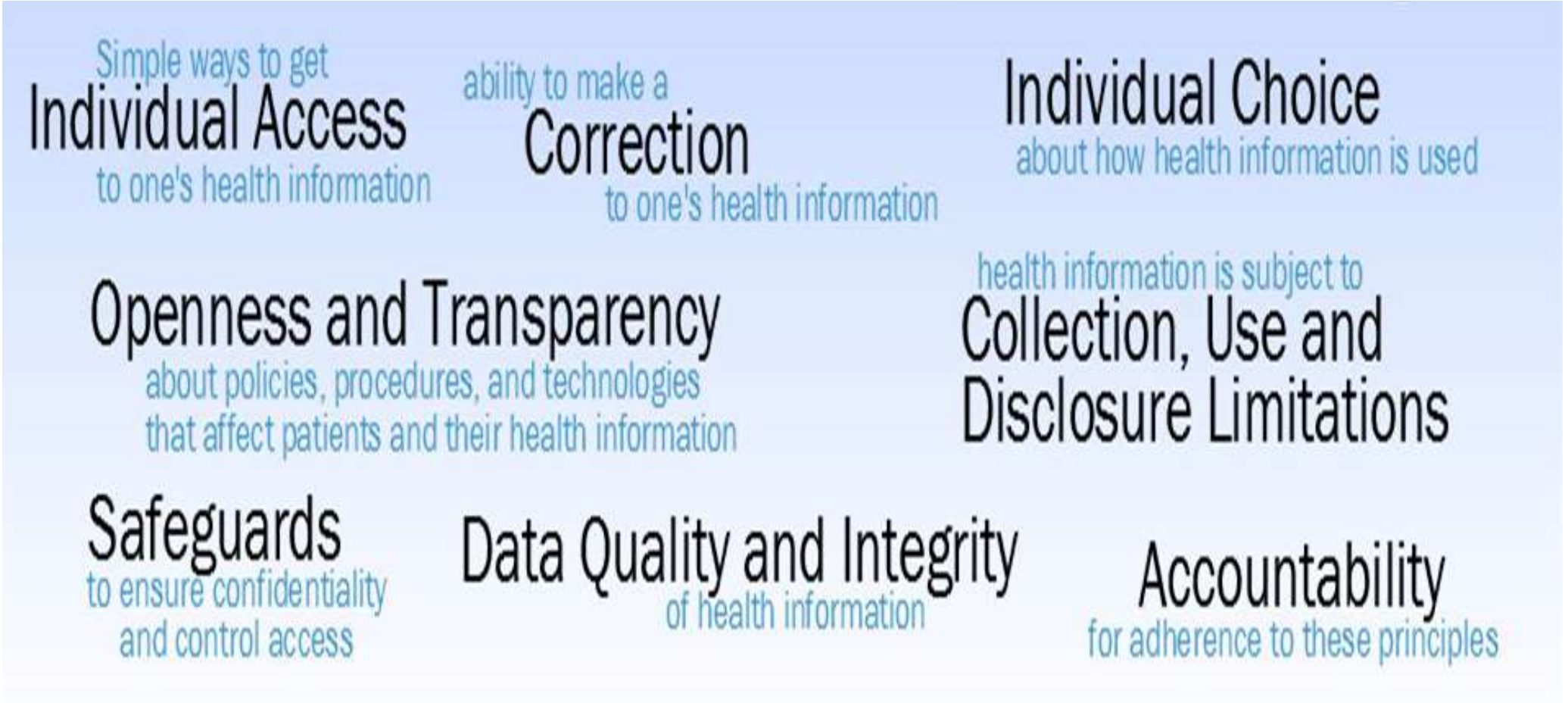
Anti-Virus (and Malware)



CyberInsurance



Maybe…Do Right, not Rights. FIPPs….



Valerie.lyons3@mail.dcu.ie
Valerie.lyons@bhconsulting.ie
Val.lyons@Hotmail.com