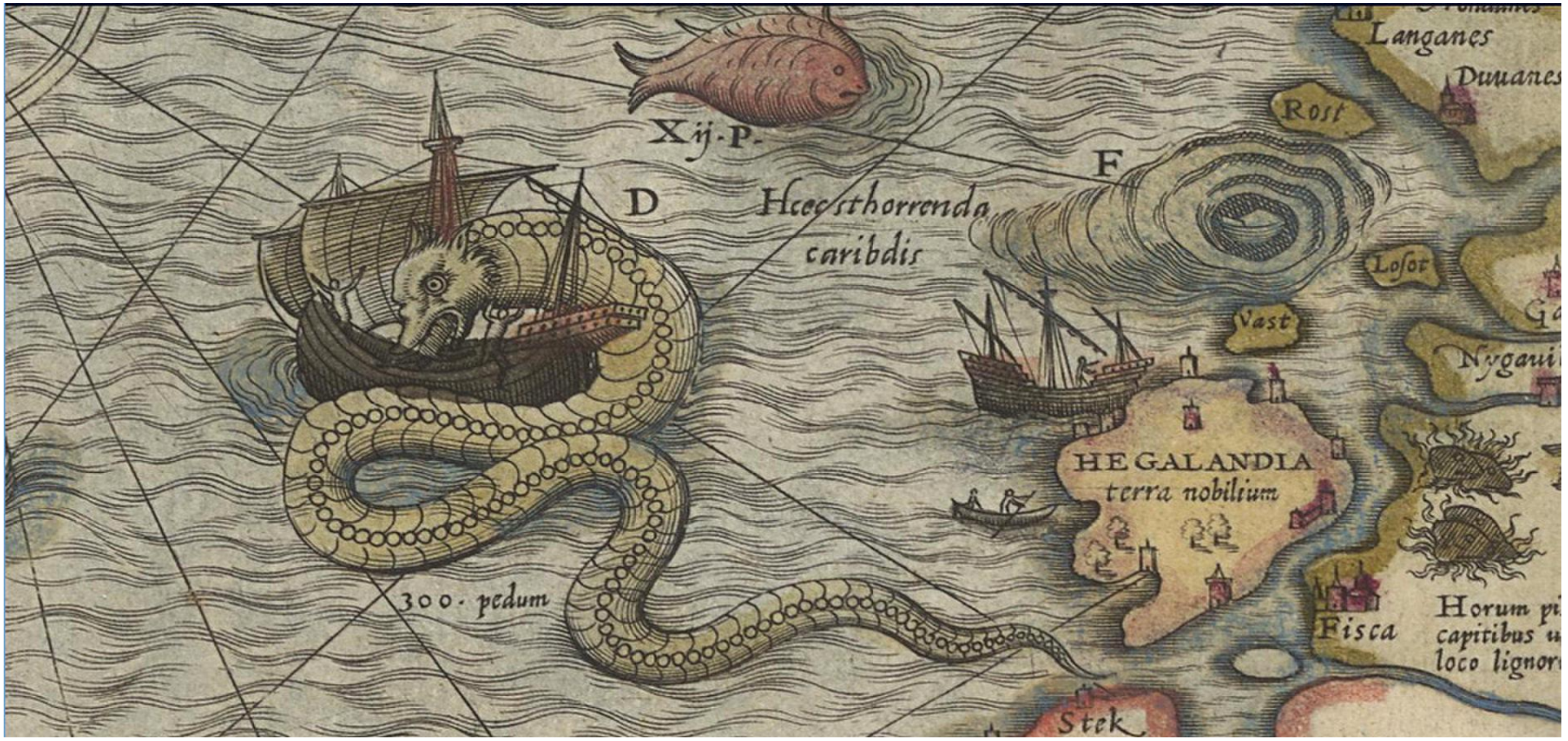
Data Protection and Freedom of Information: Two sides of the same coin

Dr Rena Gertz, Data Protection Officer, University of Edinburgh

Here be Dragons



Data Protection Law

What is personal data?

- "…any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier."
  - Structured information (only manual data)
  - Held electronically
  - About a living individual
  - Identifiable directly or indirectly
  - Online identifiers

What makes data identifiable?

Year of birth

What makes data identifiable?

Gender

What makes data identifiable?

First part of post code

What makes data identifiable?

Place of birth

What makes data identifiable?

Year of birth:	1968
Gender:	Female
First part of post code:	EH32
Place of birth:	Giessen, Germany

What is personal data?

- Structured information
- About a living individual
- Identifiable directly or indirectly

} content and context!

What is personal data

- Structured information
- About a living individual
- Identifiable directly or indirectly

Test: ‘motivated intruder’ – what is reasonably likely?

What is sensitive personal data – now called special category data?

- Racial or ethnic origins
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health data
- Sexual orientation and sex life
- Genetic data
- Biometric data

The Data Protection Principles

Fair Processing

Battersea Dogs & Cats Home

Cancer

British Heart Foundation

Pharmacy2U

Guide Dogs

IFAW

Cancer Research UK

RSPCA

Great Ormond Street Hospital Charity

WWF

University privacy notices

- The intention: avoid a patchwork of numerous little privacy notices

- Data Protection website for all things privacy notice:

Privacy notices | The University of Edinburgh

- The main University Privacy Notices:

University corporate privacy notices | The University of Edinburgh

Lawful Processing of Personal Data

- **Consent**;
- Necessary for the performance of a **contract** with the data subject including steps taken to enter into a contract by the data subject;
- Necessary for compliance with a **legal obligation**;
- Necessary to protect **vital interests**;
- Necessary for the performance of a **task** carried out in the **public interest** or in the exercise of official authority vested in the controller;
- Necessary for the purposes of the **legitimate interests** of the data controller (not public authorities in the performance of their tasks).

Consent – a ‘shoogly peg’

- Onus on controller to demonstrate valid consent has been given

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Valid Consent under the GDPR

- ✓Informed
- ✓Unbundled
- ✓Active opt-in
- ✓Granular
- ✓Named
- ✓Specific
- ✓Verifiable
- ✓Easy to Withdraw
- ✓No imbalance of power
- ✓Refreshed

Lawful Processing of Special Category Personal Data

- Explicit consent;
- Necessary for employment and social security and social protection law
- Necessary to protect the vital interests;
- Necessary for medical or social care systems if by or under the responsibility of someone owing a duty of confidentiality;
- Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

Making research lawful

- Change in legal basis – from consent to public task
- Exemption at the discretion of researchers
- Retention can be indefinite – but you have to state why

International data transfer

- **What is included:**
  - Transferring data abroad
  - Posting photos on the internet
- **What is not included:**
  - Posting text on the internet
  - UoE student or staff member travelling abroad and working on their laptop from there

International Transfers

- Personal data transfers outside of the EEA are acceptable if certain **safeguards** are in place:
  - **Adequacy status**: country treated as an EU member state
  - **DPF and Data-Bridge**: transfer to the USA
    - But: brand-new and quite a lot of work…
  - **International Data Transfer Agreement**

Data Subject Rights under the GDPR

- Subject access
- Data portability
- Rectification of data
- Erasure of data
- Object processing
- Restrict processing

Summary of Direct Marketing and the Law

				
Mail can be sent without consent. NB New Regulation may change that.	Live calls are okay unless recipient registered with TPS. If so, you need consent	Automated calls require consent.	Emails require consent.	Text/SMS messages require consent.

When consent is needed

- Required to send marketing emails and text messages to individuals
- Important: service messages/essential emails will NOT require consent!
- Required to make marketing calls if number on TPS

Soft Opt-in for individuals

- Allows direct marketing messages to be sent via email or SMS where:
  - The person has provide contact details in the course of a sale or negotiations for a sale; and
  - The marketing relates to that organisation's similar products and services only; and
  - The recipient has been given an option to opt-out at the time and every time a message is sent.
- Based on LEGITIMATE INTERESTS not consent!

Direct Marketing without Consent

- Postal and live calls
- B2B marketing:
  - E.g. getting business cards
  - Legal basis: legitimate interest
- AND you must provide the data subject with privacy/fair processing information when you obtain their data

Personal Data Breaches

- There is now a requirement to report certain personal data breaches
  - To the ICO: if there is likely to be a risk to the rights and freedoms of the data subjects
  - To the data subjects: if there is a likely to be a high risk to the rights and freedoms of the data subjects
- Within 72 hours of discovering the breach
- Obligation to keep a Register of all personal data breaches regardless of whether reported

What is Personal Data Breach?

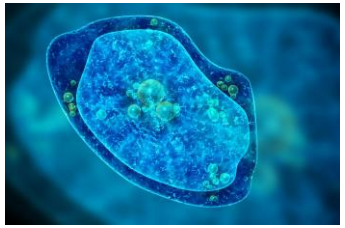
- Broader than losing data:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The other side of the coin

Who?

- Everybody can make FOI requests
- No matter the nationality
- No matter the place of residence
- “An amoeba from Mars can make a request if it can type, pick up the phone or handwrite!”
- Requests must be in ‘permanent format’.
  - Huge debate: voicemails!!



What?

- Information that is recorded:
  - Paper
  - Electronically
- Information that is held by a body on their own behalf, not on behalf of someone else
- But not your own personal data!

From whom?

- Only from public authorities (list in the legislation)
- 20 working days
- Only if request is not vexatious or repeated (can be refused otherwise)
  - "I'll keep making FOI requests to your Council until you give me a parking bay right outside my house!" – vexatious!!!

Exemptions - absolute and qualified

- Information otherwise accessible (a)
- Research (q)
- Commercial interests (q)
- Conduct of public affairs (q)
- Confidentiality (a)
- Health and safety (q)
- Personal data (a)
- Vexatious requests

Absolute: The personal data exemption

- Check:
  - Is it personal data?
  - If released, would it breach one of the DP principles?
  - Does the requester have a legitimate interest in the data?
  - Do the 'rights and freedoms' of the data subjects override that?
- Examples:
  - "I would like to know all cases of childhood leukaemia by year and census ward in Dumfries and Galloway"
  - "Give me a copy of the Committee minutes discussing special circumstance cases"

Qualified: The commercial interest exemption

- Disclosure would likely prejudice substantially the commercial interests of any person
  - "Commercial interests" = commercial trading activity within a competitive environment
  - "Likely" = significant probability that substantial prejudice would occur
  - "Substantial prejudice" = damage of real and demonstrable significance

Qualified exemptions – public interest test

- Not: What the public might be interested in!!
- Rather: Does the public interest in *withholding* the information outweigh the public interest in *disclosing* it?
- Rather:
  - Accountability for expenditure of public funds
  - Value for money
  - Performance of services

Requester doesn’t like the answer…

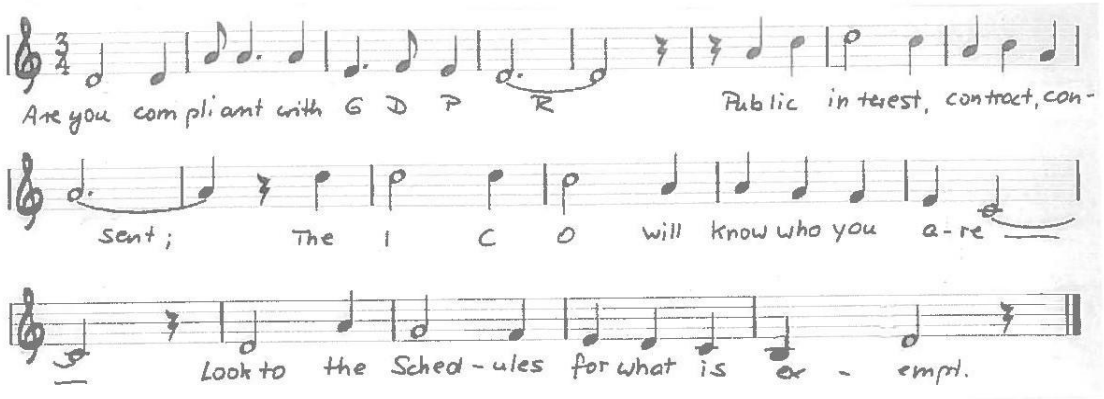
- Ask for a review!
- Then appeal to OSIC
- Then Edinburgh Court of Session
- Then Supreme Court

Homework….

Make an FOI request to a public authority (Council, Government…. But **NOT** our University!!!!!!!!!)

The Data Protection Song

(to the tune of 'Scarborough Fair')



Are you transparent in all that you do?
Public interest, contract, consent
Your privacy notice should give you a clue
Look to the Schedules for what is exempt.

Have you conducted a DPIA?
Public interest, contract, consent
To give your stakeholders all a say.
Look to the Schedules for what is exempt.

Don't process data unlawfully.
Public interest, contract, consent
Or a fine of twenty million you'll see.
Look to the Schedules for what is exempt.

With subject rights you will have to comply
Public interest, contract, consent
Access, erasure – you should not deny.
Look to the Schedules for what is exempt.