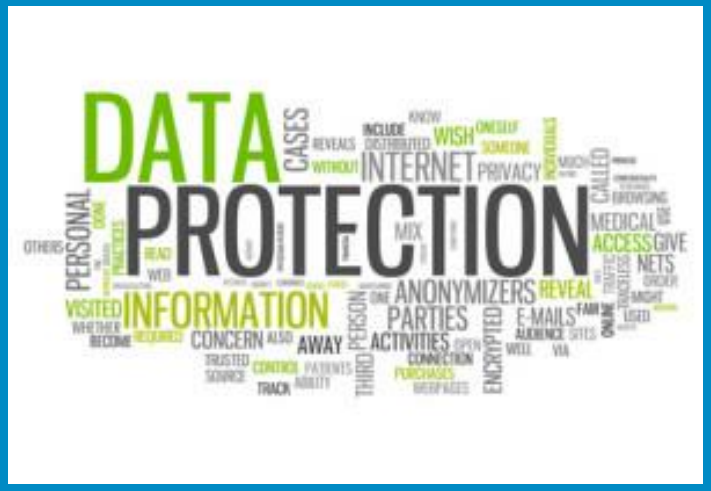

Privacy 2: Data Protection

Omid Hajilou

14 Nov. 2019





CO643/CO841

Computing Law and Professional Responsibility

University of Kent

Origins

- Hesse(n), 1970: DP regulations (in a German state)
- Sweden, 1975: first DP state law
- UK: **Data Protection Act 1984** (fear of the database state)
- OECD/Council of Europe: EU Data Protection *Directive* 1995
  => UK's partial implementation **1998 Data Protection Act**
- **GDPR**: agreed 2016 – EU law in effect since May 2018
  => UK's **new Data Protection Act (2018)**

GDPR = General Data Protection Regulations
OECD = Organisation for Economic Co-operation and Development

Data Protection Act 1998

Terminology:

- **Personal** data vs. **Sensitive** data

Roles:

- Data **Controller** vs. Data **Processor**
- Data **Subject** (living)
- **Information Commissioner** (Elizabeth Denham)

Key aim:

- Data minimisation (**adequate, relevant & sufficient**)

Was in force until May 2018, when EU's GDPR led to the new Data Protection Act (2018), even **despite Brexit**

Data Protection Act 2018

- Obtain consent
- Timely Breach notification
- Right to data access
- Right to be forgotten
- Data Portability
- Privacy by design
- Data Protection Officers (depends on size)

DP Principles

Personal information should be …

1. Fairly, Lawfully *and* *Transparently* processed
2. Processed for limited (specified) purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary *in ID-able form*
6. [Processed in line with your rights]
7. Secure against malice, loss, accident
8. [Not transferred to other countries without adequate protection] & *accountability.*

italics: new emphasis in GDPR, [ ] *modified…*

Processing… what is fair?

Essentially only allowed if…

- Part of an **agreement** (contracts)
- Necessary to **protect** (students)
- **Consent** given (*explicit, unambiguous, freely given*)
- **Legitimate** interest (limited)

For sensitive data instead…

- Legal obligation, consent or necessary to **protect vital interest** (e.g. doctors, social services)

All above applies to **electronic & paper** data (except private)

Personal liability if acting outside authority

Data subject's rights

- **Subject Access Request** (SAR) to **data & purpose**
- Rectification (**correction** or blocked)
- *Erasure (***remove** or destroy)
- Preventing processing (in case of **harm**)
- Preventing **unsolicited** marketing
- Preventing **automated** decision making (HR warning)
- **Compensation** & Complaining
- ***Transparency*** *(how is data used)*
- ***Portability*** *(switch supplier)*

Key offences and penalties

- Processing without registration
- Notification issues
- Unlawful obtaining data (e.g. Criminal Records Check)
- Forcing Subject Access Request (cautions/convictions)

Old: Penalty max **£500K** but offenders often prosecuted for related offences (e.g. misconduct in public office)

New: Penalty max **£17 million** (20 million under GDPR, in Europe), or up to **4%** of global turnover.

Consequences of data loss

Penalties were up to £500K, but under GDPR they can be up to £17 million (UK) or 4% global turnover

ico.
Information Commissioner's Office

NHS Surrey

12 July 2013

A monetary penalty notice has been served on NHS Surrey following the discovery of sensitive personal data belonging to thousands of patients on hard drives sold on an online auction site. Whilst NHS Surrey has now been dissolved outstanding issues are now being dealt with by the Department of Health.

£200,000
PENALTY

Facebook (vis-à-vis Cambridge Analytica)

25 October 2018

Between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had. Up to **87 million users** were impacted by this serious breach.

£500,000
PENALTY

However…

Is it out of your hands?

- Do Subjects know - **who holds their data**?
- **National security** exemptions remain
- Also exemptions for: crime, health, tax, social work; students; research: statistical purpose, journalism (public interest); staff planning; employment references.

Security considerations (GDPR)

Start with **Policies & procedures**; carry out **Training & Audits.**

Encryption:

- "**at rest**": encrypted backup tapes/disks
- "**in transit**": encrypted communications, web connections (HTTPS)
- not just "confidentiality" but also "**integrity**"

Anonymisation

- *Nobody* can re-identify. No longer personal (large numbers)

Pseudonymisation:

- **removing** all/most **identifying information** by a unique label per person (e.g. medical databases use link-label)
- **Danger**: if **someone has the link-label** and can access the data
- **DPA** assumed info **non-personal**, but **GDPR** considers info personal, so responsible behaviour is required (i.e. **reduces risk only**)

Access control

- Can ensure that data only accessible to **those who need to know**.

What else in GDPR?

"Regulation" means …

- Wider extraterritorial: "**doing business**" in EU
- Data Protection **impact assessments** for more risky processing
- "**Right to be Forgotten**" already in 95/98, extended a bit
- One stop shop
- Data breach **notifications**
- Privacy **by design**
- **Biometric and Genomic data** (sensitive personal data extension)

Research data and the GDPR

- (Summary, see https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/)
- Allowed to **re-purpose data for research** Art 6(4) "compatible" purpose (even sensitive)
- **Archiving**, statistics, historical research by definition "compatible"
- Generally: "Where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject", needs to meet "the reasonable expectations of data subjects based on their relationship with the controller"
- "in keeping with recognized **ethical standards** for scientific research"
- **Notifications** proportionate

Finally, the economics of privacy/personal information

Privacy Paradox: Why do we say **we value our privacy** and yet are quite willing to allow our personal information to be used for example in **exchange for obtaining 'free' services**?

Is privacy/personal information **just another commodity** for many of us?

Should we make an **exception for AI algorithms**, that benefits the vulnerable (e.g. Facebook self-harm/suicide prevention), and can we trust AI?

CO643/CO841
Computing Law and Professional Responsibility





University of Kent