Queen Mary
University of London
Science and Engineering

ECS7025P Ethics, Regulations and Laws in Advanced Data Processing and Decision Making

Week 9

Comply with the law

Mahesha Samaratunga

Learning Objectives:

- Introduction to the 3rd specific action in UK Gov's Data Ethics Framework—Comply with the law
- Develop understanding to GDPR and DPA2018 legal framework that related in the data processing.
- Build concepts on other general regulations, laws and code of practices.

Get legal advice

- Have you spoken to a legal adviser within your organisation?
- Have you spoken to your information assurance team?
- Have you consulted your organisation's Data Protection Officer when doing a DPIA?
- What legal advice have you received?

What data are we allowed to use?

As a data scientist you will be making use of a wide range of datasets to conduct your analysis. This will also involve quantitative secondary research sources that includes data such as census data, birth/death rates, unemployment rates. This type of data is normally generated by governments, organisations and charities. Which leads us to the question: *Are we allowed to make use of this data?* The answer is ‘yes’, however you need to be aware of legislations related to the usage of data. According to gov.uk, This includes how you:

- produce statistics,
- protect privacy by design,
- minimise the data needed to achieve your need,
- keep personal and non-personal data secure.

Further processing of personal data by a state body

In February 2015, we received a complaint from an employee of a state body in relation to the alleged unfair processing of his personal data. The complainant stated that, in the course of a meeting, he had been advised that his manager had requested access to data from his security swipe card in order to compare it with his manually completed time sheets. The complainant explained that this had been carried out without any prior consultation with him or his line manager. By way of background, the complainant informed us that the security swipe cards used by the employees are for accessing the building and secured areas only, and are not used as a time management/attendance system.

We sought an explanation from the body concerned as to how it considered that it had complied with its obligations under the Data Protection Acts in the processing of the complainant's personal information obtained from his swipe-card data. We also advised it that we had sight of the relevant section of its staff handbook and we noted that there was no reference to the swipe card being used for the purpose of checking attendance.

We received a response explaining that the swipe-card data relating to the complainant was handed over to the complainant's manager in good faith on the basis that it was corporate rather than personal data. The organisation also confirmed that it checked the staff handbook and any other information that may have been circulated to staff regarding the purposes of the swipe card and that there was no mention of the use of swipe cards in relation to recording time or attendance. It advised that the focus of the information circulated with regard to swipe cards was on security and access only.

After consideration of the response received, along with the content of the complaint, we informed the organisation concerned that we considered that the Data Protection Acts were breached when the employee's swipe-card details were provided to his manager to verify his working hours. We referred to the provisions of Section 2(1)(c)(ii) of the Data Protection Acts, which state that data shall not be further processed in a manner incompatible with the purpose for which it was obtained. Given that we considered the information concerned had been processed in contravention of the Data Protection Acts 1988 and 2003, we required an assurance that all email records created in relation to the further processing of the swipe-card details concerned be deleted from its systems; this assurance was duly provided.

The complainant in this case agreed, as an amicable resolution to his complaint, that he would accept a written apology from his employer. This apology acknowledged that the complainant's data protection rights had been breached and it confirmed that the organisation had taken steps to ensure that this type of error did not recur in the future.

Discuss

- From a data protection perspective, why is this a concern?

Personal data Protection

If you are using personal data, you must comply with the principles of the

- EU General Data Protection Regulation (GDPR) and
- Data Protection Act 2018 (DPA 2018) which implements aspects of the GDPR and transposes the Law Enforcement Directive into UK law.

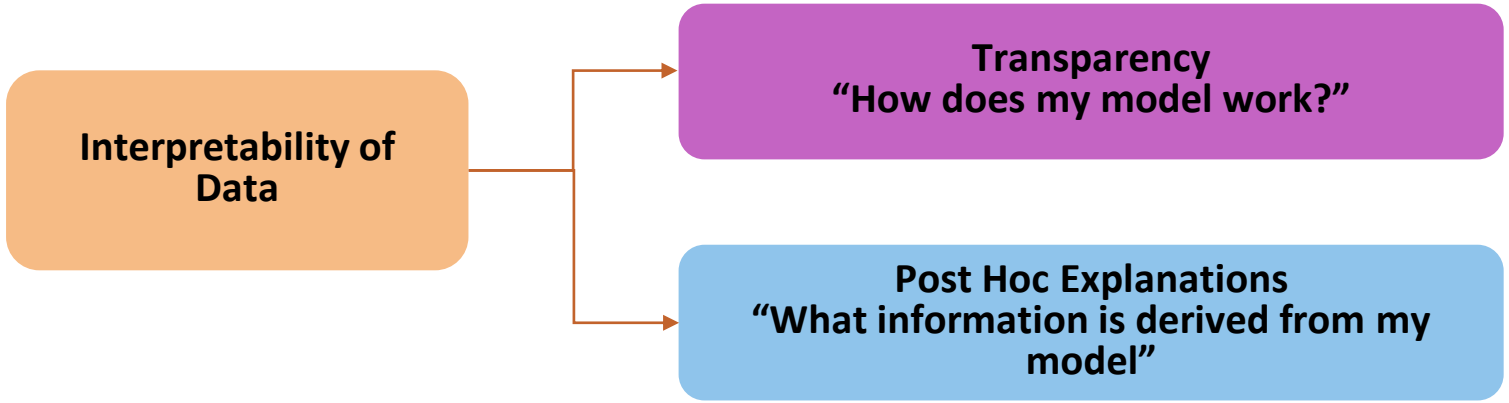
Personal data is defined in Section 3(2) DPA 2018 (a wider explanation is detailed in Article 4 of the GDPR).

- "Personal data" means any information relating to an identified or identifiable living individual
- "'personal data' means any information relating to an identified or identifiable natural person ('data subject')……; " --- Article 4 of GDPR

A Summary of EU GDPR

Data Protection Act 2018

Data scientists also need to take into consideration the interpretability of data, as this is also a GDPR requirement. There are two aspects to the interpretability of data, which are transparency and post hoc explanations. Transparency is based on how your model works, while post hoc explanations are based on the information derived from your model. From a GDPR perspective, this is important as a user has the legal right to find out how an algorithmic decision was made about them.



After class, you should read the relevant legislation documents to familiarise yourself with the legal implications:

Producing statistics - Code of Practice for Statistics

Minimising the data needed to achieve your need - Article 5(1)(c) of GDPR

Information governance - keeping personal and non-personal data secure (e.g. collection, storage, sharing and deletion) - General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018)

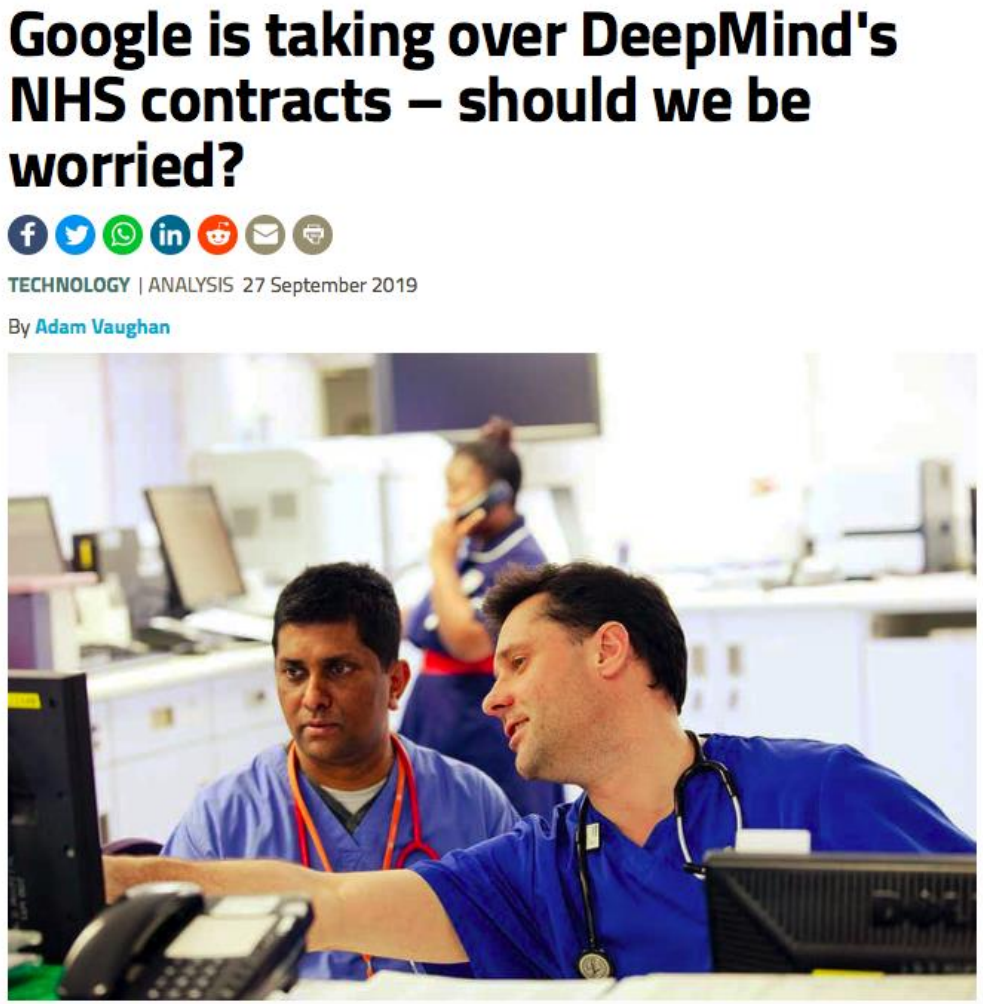
- GDPR Enforcement Tracker

GDPR case study

Read the following article and discuss the following questions:

https://www.newscientist.com/article/2217939-google-is-taking-over-deepminds-nhs-contracts-should-we-be-worried/

- Is this a privacy concern? If yes, then why?
- Are the patients obliged to share their data?



Google is taking over DeepMind's NHS contracts – should we be worried?

TECHNOLOGY | ANALYSIS 27 September 2019

By Adam Vaughan

Data protection by design and DPIA

GDPR requires that anyone handling personal data protects the rights of individuals by:

- Using personal data for a specific task
- Putting in place technical and organisational measures to implement data protection principles effectively
- Integrating necessary safeguards into the processing of personal data

It is a legal obligation under Article 35 of the GDPR to complete a **DPIA (Data Protection Impact Assessment)** when there's likely to be high risk to people's rights, particularly when using new technologies. However it is often good practice to do a DPIA for any use of personal data.

The DPIA template

DPIA

In the DPIA you must:

- Describe the nature, scope, context and purposes of the processing;
- Assess necessity, proportionality and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

Things to think about:

- Always seek the advice of your organisation's Data Protection Officer when doing a DPIA
- Privacy should be considered throughout the project – although you may not be using personal data at the outset of your work, the project type and privacy considerations may change as work develops
- Consider how often you will repeat the DPIA when using personal data and may need to change this if the project changes significantly
- When joining a new project, seek out and review the existing DPIA to familiarise yourself with any risks to rights and freedoms identified and the relevant mitigation strategies proposed
- If you discover a DPIA has *not* been completed for a project for which it is relevant, this should be flagged as soon as feasible
- Refer to the ICO's guidance on DPIAs

Legal Liability

Decision making models are dependent on data that is generated given a particular scenario. One such example is the series of decisions that have to be made given the data captured by the multiple sensors in Autonomous Vehicles (AVs). The question that we need to think about are:

“Who makes these decisions?”

“Are there any legal liabilities for these decisions?”

Scenario 1

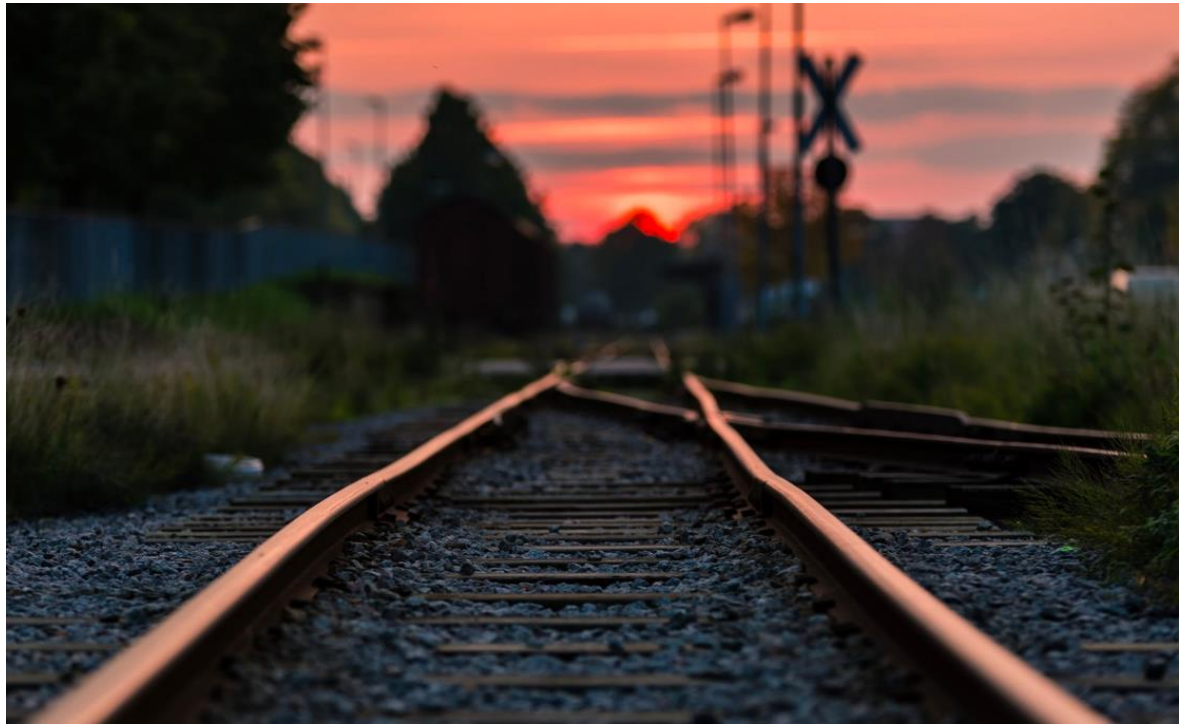
Imagine a runaway train is madly hurtling towards 5 people on a railway track – you look around but there's no way of warning them.

You notice that you're standing next to a lever that operates some points – you can divert the train onto another track and save the people – hurrah!

But there is a problem – there is also a person on the other track. If you hit the lever and divert the train then they die.

If you do nothing then 5 people die, but if you pull the lever then 5 people are spared but 1 person dies.

What would you do?



Scenario 2

Now let's change some of the conditions and look at this again. Imagine the train heading for those 5 people again. This time though, there are no points – but there is a very very large person on a bridge above the tracks.

You realise that the only way of saving the 5 people is to push the large person onto the tracks, just as the train approaches. They would die, of course, but the 5 would be spared. I mean, you have to suspend some disbelief here – the person would have to be huge to stop a train!

Similar ethical dilemmas happens to designing autonomous vehicles algorithm.

Will the legal liabilities be the same for a pre-programmed AV and a human-driven car?

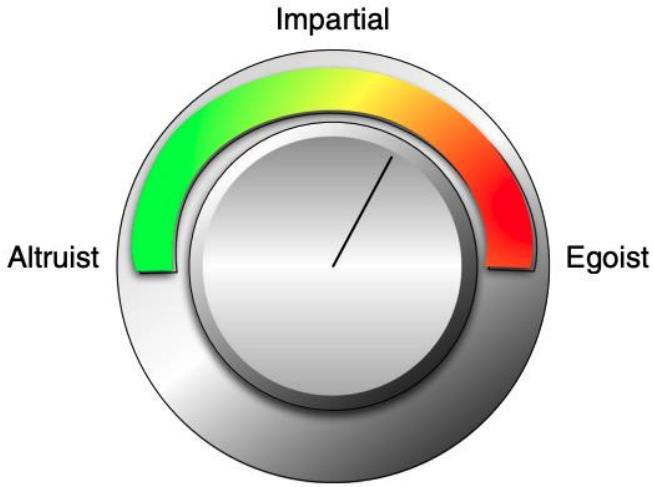
Read the article: ‘The Ethical Knob: ethically-customisable automated vehicles and the law’ and discuss the following questions:

Who takes the legal liabilities for:

- Human-driven car
- Pre-programmed AV
- Ethically-customized AV

What are the impact of Ethical Knob? Is it needed?

Menti.com 96 66 37 1



Accountability & Transparency

Article 5(2) of the GDPR says:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Art. 30 GDPR

Records of processing activities

1. [1] Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. [2] That record shall contain all of the following information:

Publish your DPIA and other related documents

Equality and discrimination

Analysis or automated decision making must not result in outcomes that lead to discrimination as defined in the Equality Act 2010.

Information governance

- Organisations have a responsibility to keep both personal data and non-personal data secure.

- In many organisations information risk is (should be) overseen by a Senior Information Risk Owner (SIRO). Usually your organisation will have a risk appetite statement that sets out how information risk is managed.

- Consult with your information assurance team when you need to delete data.

Sharing and re-use of data

- When accessing or sharing personal data, you must follow the Information Commissioner's Code of Practice for Data Sharing which should be read alongside the ICO's guide to GDPR. This code of practice has been updated in December 2020.
- When accessing and sharing data under powers in Part 5 of the Digital Economy Act 2017, you must follow the relevant codes of practice.
- When re-using published and unpublished information relating to public tasks, you must follow the Re-use of Public Sector Information Regulations 2015.

Copyright and intellectual property

Copyright and (Intellectual Property (IP) are often governed by combinations of statutes.

- When using data, respect copyright laws and database rights, covered in part by the Copyright and Rights in Databases Regulations 1997.

- When procuring software, consider potential intellectual property constraints covered in the Intellectual Property Act 2014.

Freedom of information

- The use of data may be subject to the Freedom of Information Act 2000.

- Also consider the wider publishing of datasets released following a Freedom of Information request, in accordance with the Protection of Freedoms Act 2012.

Sector specific legislation

Specific sectors like finance and health have further data use legislation and frameworks, including those relating to the use of non-personal data.

- Health research has its own UK Policy Framework for Health and Social Care Research drafted by the NHS Health Research Authority (HRA).
- The NHS HRA also provides specific guidance for health researchers on the new data protection principles being introduced by the GDPR.

Other regulations, laws and code of practices in UK

Other important pieces of central government guidance that are helpful for using data and designing projects in the public sector include:

- The Civil Service code
- HM Treasury Aqua Book: guidance on producing quality analysis for government
- HM Treasury Magenta Book: guidance for evaluation

Queen Mary

University of London