1. History of European Data Protection Law

a) Purpose

- Advancement of technology has led to increase in collecting, storing and analysing peoples' data
- Risk of misuse, and damage to people due to misuse of information has increased

b) Instruments giving an impetus to create Data Protection Laws

- Universal Declaration of Human Rights (1948)
  - Art. 12: right to private life
  - Art. 19: right to freedom of opinion and expression
  - Art. 29(2): where conflict between rights, a balance has to be struck

- European Convention on Human Rights (1953)
  - Council of Europe invited states to sign ECHR
  - Only applies to member states of Council of Europe (NB: this is an organisation that is separate from the EU)
  - The ECHR is enforced by European Court of Human Rights
  - Art. 8: right to private life
  - Art. 10: right to freedom of expression
  - these rights are qualified i.e., can be infringed upon in the interest e.g., national security, territorial integrity or public safety, …

- Treaty of Lisbon (2007)
  - amends Treaty on European Union and Treaty on the Functioning of the European Union
  - Art. 16(2) of TFEU provides that European Parliament and Council, acting in accordance with ordinary legislative procedure, shall lay down rules relating to protection of individuals with regard to data processing

- Charter of Fundamental Rights of the EU (2009)
  - Article 8 provides the following:
    - *1. Everyone has the right to the protection of personal data concerning him or her.*
    - *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
    - *3. Compliance with these rules shall be subject to control by an independent authority.*

c) Timeline of Data Protection Laws

- Between 60s-80s, several European countries were early adopters of data protection laws, including Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Sweden and Norway
- 80s: OECD created "Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data" (not binding)

    - Application: processing of personal data that due to the nature or context of processing, pose a danger to privacy and individual liberties
    - Core principles:
        - Collection limitation - collection of personal data should be limited and done in a lawful way
        - Data quality - personal data retained should be accurate
        - Purpose specification - purpose of collection should be communicated at the point of collection and not deviated from
        - Use limitation - personal data should not be disclosed or used for purposes other than those communicated
        - Security safeguards - personal data should be kept securely
        - Openness - there should be policy of transparency as to what happens with the personal data
        - Individual participation - individuals should have right to obtain personal data
        - Accountability - data controller should be accountable for complying with the requirements above
    - International transfers: member countries should take steps to ensure international transfers are uninterrupted and secure
    - National implementation: member states should establish laws that provide for data protection
    - International co-operation: member states should cooperate and exchange information in relation to application of these guidelines
- 1981: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - shorted to Convention 108 (binding only on states that are signatories) - was last updated in 2018 to Convention 108+ and is still present and binding on signatories
    - Convention 108+ can be accessed and reviewed here - as you will see, there are plenty of similarities with the GDPR
- 1995: Data Protection Directive (binding on EU member states, but can implement objectives how they wish)
- 2018: General Data Protection Regulation (replaced Directive; binding on EU member states and directly applicable (i.e., not flexibility for member states how to implement)

d) Data Protection Directive vs General Data Protection Regulation

- Distinction between directives and regulations in EU law generally:
    - Directive = legislation applicable to EU member states that contains objectives which member states have to achieve; member states may choose how these objectives are achieved
    - Regulation = legislation that is directly applicable to EU member states and must be implemented as is
- Reason for GDPR replacing the Directive is because member states' diverged in their approach to data protection law, making compliance stemming from cross-border data processing and transactions difficult

- Key changes introduced by GDPR include, but are not limited, to the following:
    - stronger rights for individuals whose data is processed by organisations
    - requirement that data privacy to be taken into account when new technologies developed
    - introduction of concept of accountability
    - increased powers for supervisory authorities

- concept of one-stop-shop (meaning that organisations can deal with a single lead supervisory authority for most of its processing activities)
- broader applicability of GDPR to anyone targeting EU consumers

e) Related Legislation

- The Law Enforcement Data Protection Directive
  - relates to processing of personal data by competent authorities for purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties and on free movement of such data
  - does not preclude member states from providing higher safeguards in their national law to protect rights of data subjects
- The ePrivacy Directive
  - sets out rules about processing personal data across public communications networks, e.g., e-mail communications
  - Includes for example stringent rules about website visitors providing consent before cookies can be used, e-mail marketing, etc.
  - as of early 2023, an ePrivacy Regulation has been drafted and is currently in the process of being approved within the EU - once in force, the ePrivacy Regulation will replace the ePrivacy Directive

f) Brexit

- After 31 December 2020, the UK is no longer part of the EEA
- UK incorporated EU GDPR creating a separate UK GDPR
- Adequacy decisions granted in respect of each other, meaning that
  - EU data can flow to UK
  - UK data can flow to EU
- Further, UK will
  - permit transfers from UK to EEA and Gibraltar
  - permit transfer subject EU Commission adequacy decision
  - permit transfers based on EU data protection clauses
  - recognise existing binding corporate rule approvals
- 2 separate legal frameworks which may diverge in future

g) Convention 108+

- Signatories: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108
- Parties must give effect to provisions via law
- Data processing shall be proportionate, on a lawful basis (such as consent), processed fairly and collected for specific purposes, accurate, preserved in a form permitted identification
- Special categories of data can only be processed where appropriate safeguards present; special categories include:
  - Genetic data;
  - Personal data relating to offences, criminal proceedings, convictions, related security measures;
  - Biometric data; and

    - Personal data revealing racial, ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.
- Requirement to take appropriate security measures
- Certain information need to be provided data subject e.g., identity, legal basis of processing, categories of personal data processed
- Data subject rights
    - Not be subject to automatic decision making;
    - Obtain on request confirmation of processing;
    - Object to processing;
    - Obtain rectification;
    - Have a remedy where rights are violated;
    - To benefit from assistance of supervisory authority based on nationality or residence;
- controller must notify, without delay, at least the competent supervisory authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects
- Exceptions and restrictions from certain obligations where necessary e.g., for national security
- International data transfers must provide adequate protection to data subject's personal data
- Key differences to Convention 108:
    - Introduction/expansion of certain data processing concepts e.g., proportionality, lawful basis etc.
    - Broadening of application to both automated and non-automated processing
    - Broadening of types of special categories of data, which will now include genetic and biometric data, trade union membership and ethnic origin.
    - Requirement to notify of data breaches
    - Information obligations leading to greater transparency
    - Stronger accountability of data controllers
    - Requirement that the "privacy by design" principle is applied
    - Application of the data protection principles to all processing activities
    - Stronger requirements in relation to trans-border transfers - appropriate safeguards must be in place