CHAPTER II
PROTECTION OF DATA AND GENDER MINORITY IN EUROPEAN UNION

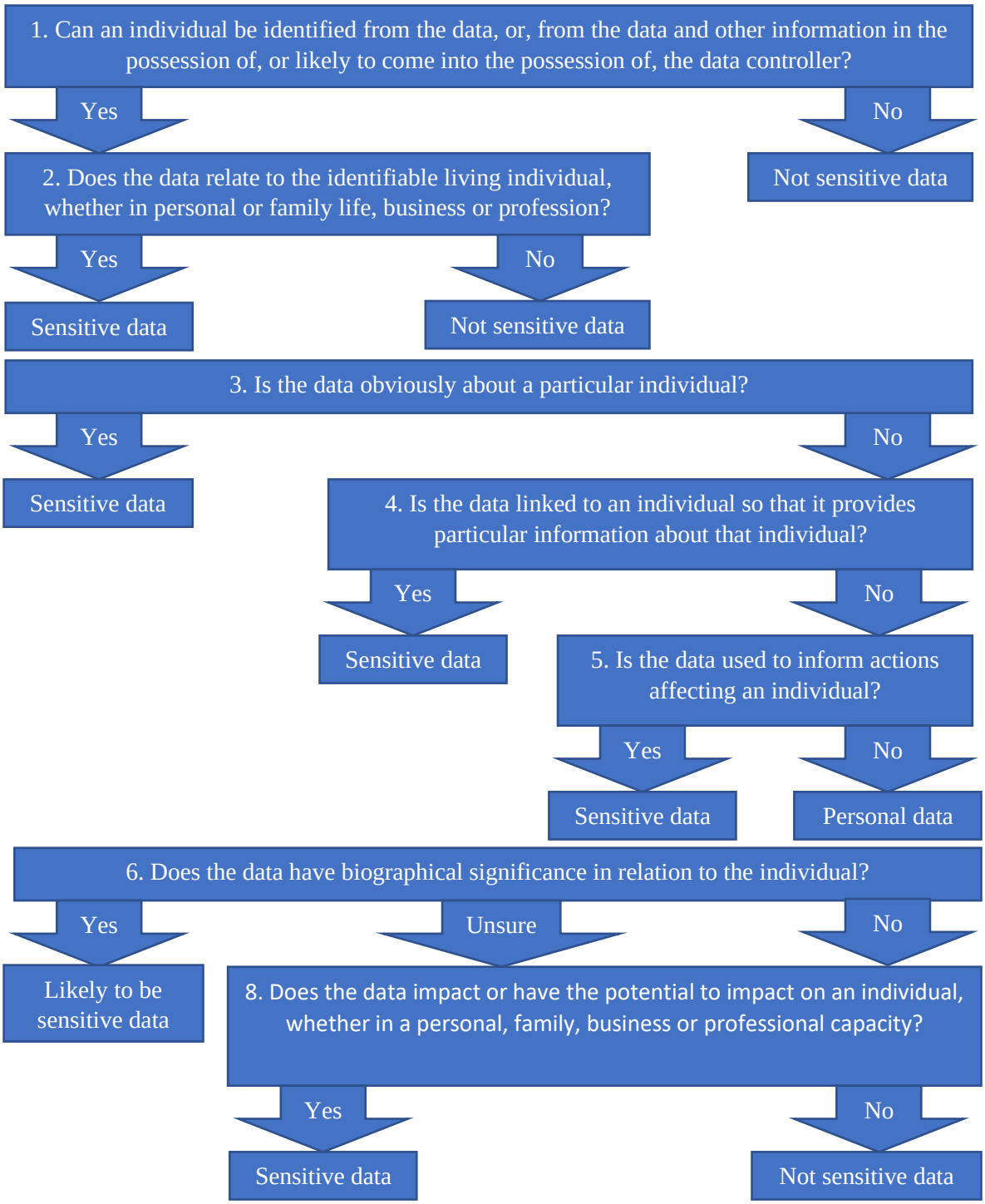
2.1 Data and the Protection Policy of Data in Cyberspace by European Union

Data protection law or policy refers to the legal scheme of the governance from gathering, preserving, processing, disclosing, and transferring of individuals' personal data online and offline. In Europe, that is recognized as a leader in data protection, this legal scheme protects individuals' basic right to privacy, generally, and basic right to data privacy, specifically. The rights to privacy and data privacy are guaranteed in 2 supranational conventions, namely the European Convention for Human Rights and also the Charter of Human Rights. Additionally, these rights are implemented by individual European member states, the Council of Europe, and also the European Union. Any private or public actor that attempts to gather, analyze, or gain from the personal information of Europeans should understand European data privacy rights. (McCarty-Snead & Hilby, 2013, p. 3).

Privacy within cyberspace such as, but not limited to, anonymity, confidentiality, secrecy, and encryption is potentially covered the sources of tortious misconduct, criminality, incivility, surveillance, and threats to public health and safety. Moreover, cyberspace makes data of individuals to be tracked and traced by government, big business, and employers (Allen, 2000, pp. 1177–1186).

Data protection not only covers those within real-world but also within cyberspace. The existence of data protection policy is paramount, knowingly that there are personal data and sensitive data within cyberspace, moving and used by different actors. Personal data is all information that is relating to an individual. Collection of information, which is assembled together so that it can lead to the identification of certain people, is called personal data. Personal data that has been disguised, encrypted or falsified but can be used to re-identify someone can still be considered as personal data and fall within the scope of the law (European Commission, n.d.). To determine whether something is considered personal data or not is shown through below.

Figure 2.1.1
Sensitive Data Determination



Source: Mondaq, 2007

As shown in Figure 2.1.1 above, Mondaq (2007) has explained extensively on how to determine one's data is a sensitive data or not. First, if an individual's personal, family, business or profession can be identified through its data then it is considered sensitive data. Second, if the data is identifying to a particular individual, provides information of a particular individual and/or affecting a particular individual then it is considered a sensitive data. Thirdly, if the data has biographical siginificance in relation to the individual it is most likely to be sensitive data. Lastly, it the data has at least a potential to impact an individual, whether in a personal, family, business or professional capacity then it is considered as sensitive data. In the European Union, the protection of data is considered as part of human right and has been encased in several regulatory texts. This was done after World War II to prevent Europeans personal data being used to segregate populations and targeted minorities happening very massively again (Robinson et al., 2009, p. 6).

Data Protection Directive, hereafter DPD, is one of the closest things to law that has been around EU for some time, since 1995 to be exact. Closest thing to law because a directive is not directly applicable law in EU system, it is sort of a guidance for member states to enact its own legislation. The main objective of DPD is to balance between the protection of the right of privacy and the free movement of data. Altough it is not as strong as law, because according to Article 5 it states that member states could determine the precise conditions on how to lawfully process a personal data (Maxeiner, 1996). In 2018, after being a subject of debate by European institutions, the new regulation was effectively applied and it is called General Data Protection Regulation, hereafter GDPR. This new regulation is what we may know as law, because it is directly applicable and member states does need to create additional domestic legislation. Moreover, GDPR can actually override contrary member states law thus guaranteeing higher level of harmonization across EU (Burri & Schär, 2016).

According to General Data Protection Regulation of European Union, the processing of sensitive data will only be lawful if it satisfies at least one of the following conditions: (1) Explicit consent has been given by the data subject, unless reliance on

consent is prohibited by EU or Member State law; (2) Necessary for the carrying out of obligations under contract, employment, social security or social protection law, or a collective agreement; (3) Necessary for the establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity; (4) Necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent; (5) Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures; (6) Necessary for archiving purposes of legitimate interest, in the public interest, or scientific and historical research purposes or statistical purposes; (7) Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent; (8) Data manifestly made public by the data subject; (9) Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional; (10) Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices (Burges Salmon, 2016).

2.2 Unlawful Processing of Personal and Sensitive Data in European Union

In European Union, data misuse of data or the unlawful processing of an individual's data has been subject of debate and scrutiny of several Member States. Several cases that happened in the past years are including: unlawful processing of data in United Kingdom, hereafter UK, referendum on EU membership, and one of the largest is the scandal of Cambridge Analytica which not only become a prominent case in United States at the time of presidential election 2016, but also throughout EU.

Cambridge Analytica, which is a company based in UK, had been using data gathered by Global Science Research, hereafter GSR, developed by Aleksandr Kogan. GSR harvested up to 87 million global Facebook users' data, including 1 million UK citizens, 300,000 German citizens, and 214,000 Italian Citizens. The data that might be collected are including: public profile such as name and gender, birth date, email addresses, tagged photos, liked pages, posts, friends lists, and – to some extent – their friends data (Information Commissioner's Office, 2018; Privacy International, 2019).

According to Information Commissioner's Office (2018) Cambridge Analytica breached the law when processing those data because of the data subject is unaware that their personal and sensitive data, and their friends', was being given by Facebook to Cambridge Analytica and would be used for the purpose of political campaigns while also drawing inferences from the data subjects' political opinions, preferences, and voting behavior; which is considered sensitive data.

Another case that shows an unlawful use of personal data is shown in when Eldon Insurance, a UK based insurance company, shared several customers' personal data such as email addresses to the people working for Leave.EU[1]. The data is wrongly benefitted both parties, because Leave.EU can accessed email addresses of Eldon Insurance customers, which they exploited by sending more than 1 million emails offering discount for Leave.EU supporters that might interested in buying one of Eldon Insurance programs named GoSkippy (Information Commissioner's Office, 2018, pp. 46–48).

In the same report, it is found that Emma's Diary, UK pregnancy and childcare company, had unlawfully collected and sold personal data belongs to more than 1 million people. The data then being sold specifically to the UK Labour Party for the benefits in profiling in 2017 run-up General Election. It is considered unlawful because

[1] Leave.EU is a political campaign group that supported UK withdrawal from EU in 2016 referendum, accessed at: https://web.archive.org/web/20151013010834/http://leave.eu:80/en/our-campaign

the company did not disclose that the personal data would be used for political marketing or by political parties (Information Commissioner's Office, 2018, p. 60).

2.3 Discrimination Data Collection of Gender-Minority in European Union

European Union Agency for Fundamental Rights, hereafter FRA, released a report on difficulties face by gender minority individuals in EU. Respondents, comprised of 93,079 individuals identified as part of gender minority community, collected between April and July 2012 shows a comprehensive look of gender minority individuals live experiences; it is currently the largest of its kind and represents the widest picture available (European Union Agency for Fundamental Rights, 2014, p. 23).

Under the report released by FRA, discrimination is the highest threat faced by gender minority individuals. This further worsen by the fact that discrimination on the grounds of sexual orientation is the second highest across EU behind that on the basis of ethnic origin. Over half people, 51%, surveyed by Eurobarometer (2008) think that discrimination on the grounds of sexual orientation is widespread, compared to the 41% who think that it is rare (Eurobarometer, 2008, p. 10).

As FRA shows that many discriminations happen in the life of gender minority individuals, it is more prominent to know the data on this discrimination faced by gender minority individuals is collected and further giving policy advice to Member States in tackling discrimination problems. Data on this matter usually collected by what is called National Equality Bodies (NEB) or other states institution as mandated by EU or Member States laws. To see that, Appendix 1 helps author to sees and determines data is collected by EU Member States institutions already in line with the regulation such as GDPR to ensure to protections of gender minority sensitive data.

All EU Member States have NEB, which one of the mandates is to record and cover discrimination cases. The difference comes when each Member States have its own mandate whether to cover the issue of discrimination regarding gender minority,

such as discrimination based on sexual orientation, gender expression, and/or gender identity (Bell, 2017, pp. 9–10). The full list of EU Member States NEB could be accessed in Appendix 1.