Data Access and regulation

Exam - 04 December 2020

Course: Data Science and Economics

Name: Andrea Ierardi **ID:** 960188

Scenario 1

For what concern the Automated decision-making and profiling, individuals have the right not to be subject to a decision that is based solely on automated processing. However, there are some exceptions to this rule, such as when they have given their explicit consent to the automated decision. Except where the automated decision is based on a law, your company must:

- inform the individual about the automated decision-making
- give the individual the right to have the automated decision reviewed by a person
- give the individual the opportunity to contest the automated decision

If a bank automates its decision of whether or not to grant a loan to a certain individual, that individual should be informed of the automated decision and given the opportunity to contest the decision and request human intervention. So Anna could ask to the UsualBank's customer support if they had any trouble with the automatically request, but they are not answering her calls, so they are not conform with the Automated decision-making and profiling. Also at any time, the customer may withdraw their consent for the use of their data and this must be put on the record by banks. The customer should also have easy way to do so. Data subject can start complaining with two entities: DPO (data protection officer) or Supervisory authority.

For what concern GreenBank proposal, Anna should open a new account in the new bank first in order to move the checking account. Anna should give the permission to the GreenBank to manage her records. Consent must be clear, specific and informed. For making the contract, GreenBank need all these Anna information.

Scenario 2

We are dealing with a case of transfers of personal data to third countries and also dealing also with Big Data Analytics.

1. First, Decide if the potential contract involves personal information and what falls under the definition of personal information.

I would discuss with Nude how they manage the data. If they consider the costs of implementation and the nature, scope, context and purposes of processing and if they ensure a level of security appropriate to the risk including:

- Pseudonymisation and encryption of personal data
- Confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of incidents
- A process for regularly testing measures for ensuring the security of the processing.

Under the GDPR, Article 15 an individual has the right to ask a controller for confirmation of whether or not they are processing their personal data and if they are, access to that personal data together with a plethora of additional information.

Furthermore, all that Big Data being collected will have to not only be stored securely but will need to be gathered by customers who want to remove it and switch it over to another vendor. Businesses of all sizes will need to come to terms with the idea that customers will gain greater control over their own personal data. The right of erasure, rectification, restriction of processing and portability.

2. Second, Define whether the use of personal data falls under the jurisdiction of the European Union.

After all these conditions internally of the Nube company, we can now consider the data transfers problem. It is necessary to check whether the data transfer itself must be legal. If the intended data transfer meets the general requirements, one must check in a second step whether transfer to the third country is permitted. Any processing of personal data is prohibited but subjected to the possibility of authorization.

The GDPR will apply to the potential contract if one of the following is relevant:

- One of the contracting parties is established inside the European Union
- The involved personal information was collected because of the offering of goods and services to the EU citizens (or other people, who permanently live in the EU) or the intentional monitoring of the EU citizens information.

All third parties that receive the data shall uphold the same level of obligations the contracting parties have regarding the concerned information. The should be no problem for data transfer for Germany, since the GDPR provides, as key objective, for the free flow of data within the European Union Restrictions or prohibitions are forbidden (if data ensure a level of security appropriate to the risk). For third countries are subject to an Adequacy Decision. In this case, both Israel and Mexico have been declared adequate. They should move quickly to implement a proper compliance program and avoid the possible harsh penalties.