**Introduction:**

In the past years, more and more people have been using the internet to accomplish their daily activities, which ranges from playing online video games to paying taxes, but also some activities which were done locally are now done on far located servers (storage of data in the cloud and editing documents on Google docs are good examples of that), this threatens our privacy and ...,in fact more than 250 Million people now use the internet daily in Europe, it is thus increasingly important to protect these users and their data from misuse by the companies who they have given it to which could use it for purposes other than what the user consented to or by criminal organizations who could sell user’s data or try to blackmail them in case it would contain sensitive informations.

When looking at the recent history, we can see that many data breaches happened in the last years, from the Sony security breach in april 2011 which compromised the accounts of 77 million users to the Yahoo! breach which happened in late 2014 but was only revealed to the public late september 2016. The compromised information included names, email addresses, dates of birth and telephone numbers of over 500 million people.

These problems related to their data worries many EU citizens, when asked 71% of Europeans said that they feel that there is no alternative other than to disclose personal information if they want to obtain products or services and only 15% feel they have complete control over the information they provide online; one in three people (31%) think they have no control over it at all [?].

That is why the European Commision has proposed as early as 2012 the **General Data Protection Regulation (GDPR),** which was adopted on the 27th of April 2016.

The GDPR has set as goal to give people confidence in the online services they are using by having more transparency about how and why the data is handled. Some of the main issues addressed in the new regulation are the need for the individual’s clear consent to the processing of the personal data, the right to data portability from one service to another and the right to erasure, rectification and the new concept of “the right to be forgotten”, all of which will be explained in detail in the latter sections. it’s supposed(?) to be a modernisation and a harmonization of the actual data protection laws. It will take effect on the 28th of May 2018 and will replace the data protection directive (officially *Directive 95/46/EC*) from 1995.

The new data regime will be applied to all companies processing data for EU residents which means it will also be applied to non EU companies, In fact the new regulation will make it easier for non EU companies to enter the european market by having a harmonization of the regulation throughout the EU, instead of having them to comply with a different set of laws in each country. This is a big change from the last framework, under this regime the important thing(?) is where the company’s activity occurs not it’s location.

Before the new regulation takes effect, each company has to make sure that the way it processes their customers data complies with the GDPR. In order to do that, they must first document what data is necessary in order to serve the user and the way the data is used either by the company itself or by a third party. The company processing the data must determine whether the information is subject to the regulation.

There are strict penalties for companies not complying to the laws,they vary from 2% of the worldwide turnover (or 10 Millions €, whichever is greater) to 5% of the worldwide turnover (or 20 Millions €, whichever is greater).

What we have tried to do in this project is taking a real company as an example to illustrate how the new regulation will affect its activity and the measures it will need to take in order to comply with the GDPR, this example is rejsekort. We have therefore found how they use their client’s data in a document released by them in 2014 which can be found in the appendix.

------------------------------------------------------------------------------------------------------------------------

***get machine readable format :*** Also called data portability, it means the ability of the user to get all his data from the online service he is using in a format that is compatible with other platforms, it requires common technical standards to allow the transfer from one data controller to another. "Controllers must make the data available in a structured, commonly used, machine-readable and interoperable format that allows the individual to transfer the data to another controller." [x]. This is a change in paradigm, in fact this law means that it is the user that is the creator and owner of the content he or she is sharing on online platforms.

***Request from opinion research institutes :*** this ?

***Send data to opinion research institutes :*** Rejsekort sends users data to opinion research institutes upon request, the data includes the name, the address and the email.

It is done in order to carry out customer satisfaction surveys and improve the user experience. Only users who have agreed to share their data and have given an explicit consent will have their data used.

***Request information modification :*** Every user have the right to change the information the company has on him or her, it could be done in order to rectify the information or for any other reason the user see fit.

***Modify information :*** Rejsekort will only modify information of its users upon request.

***Right to be forgotten :*** Also called “right to erasure” is the right for the data subject to have his or her data erased and no longer processed under certain circumstances, which include :

- The personal data is no longer necessary to serve the user in relation to the purposes for which the data was collected.

- The data subject withdraws his or hers consent.

- The personal data was unlawfully used.

- The data subject has given his or hers consent as a child, without being fully aware of the consequences.

If a data subject has requested to exercise his or hers right to erasure, and it was evaluated as a legitimate request, the company has to contact all third parties (?).

The request could also be rejected if the deletion of the data would diminish the freedom of expression and information of a third party, if the data is processed for public health purposes and the public interest (?).

[x]http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL