**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 and shopping, but also some activities which were done on their own computers are now done on far located servers (storage of data in the cloud and editing documents on Google docs are good examples of that), these new ways of computing raises many questions about how our data is processed and stored, 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 company must ensure that they give data subjects clear and transparent notice of the ways in which, and purposes for which, their personal data will be processed, the right to data portability from one service to another, the right to erasure and rectification, all of which will be explained in detail in the latter sections. it is 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 offering goods and services to EU residents or monitor their behaviour 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 factor is where the company’s activity occurs not it’s location.

There are strict penalties for companies not complying to the laws,they vary from a simple written warning in case of first and unintentional non compliance to different fines.

Data controllers have to ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". Data controllers can be fined to the height of 05% of their worldwide turnover (or 20 Million € whichever is greater).

In contrast if data processors breach their statutory data security obligations, which requires them to "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" of their personal data processing, then the most they could be fined is up 02% of their worldwide turnover (or 10 Million € whichever the greater).[z]

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 the different processes and requirements to have an overall view of the system. Then, all data processing activities must be reviewed, and the company has to evaluate whether the EU regulation applies to that activity, this will allow companies to figure out which data processing activities needs to be changed, and furthermore how to implement these changes in order to comply with the regulation. The GDPR applies only to activities which process personal data. Personal data means any information to an identified or identifiable person, who can be identified either by name, social security number, location data or other. The company also has to ensure that they have a lawful basis for each personal data processing activity. A lawful basis could be an explicit consent given by the data subject, a legal obligation to perform such processing, or that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

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.

requirements :

accountability

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

***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.The right to data portability is provided by Article 18 of the GDPR.[y]

***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 (?).

***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 sees fit.

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



We can see from the figure 3.5 that “Get machine readable format”, ”Request for information modification” and the “Right to be forgotten” are excluded. There is an inclusion relation between the “Register” activity and the mentioned activities, which means that they can be executed only after “Register” has been executed. In this concrete example it means for example that a user cannot exercise his right to be forgotten before he has registered as a client.

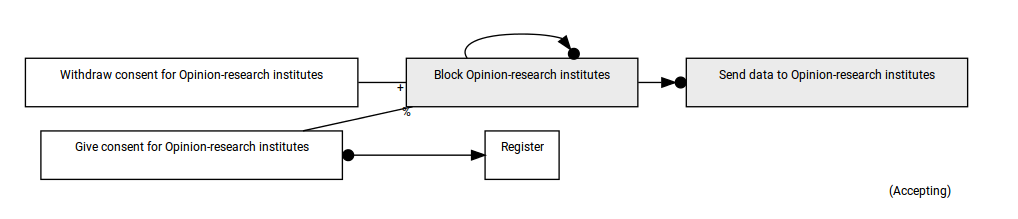
***Send data to opinion research institutes :*** Rejsekort sends users data to opinion research institutes upon request, the data includes the name, the address and the email.

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.

***Give consent for opinion research institute :*** Rejsekort will need the explicit consent of the user for each purpose it is going to use the data for. The data used include name, address and email address. The opinion research institute will delete the received personal data when they have completed their task. This consent is not mandatory in order to use rejsekort, but if given will help improve the overall service.

***Withdraw consent for opinion research institute :*** The data subject can, if he or she has previously given a consent to the company sending personal data to an opinion research institute, withdraw the consent for that processing without any justification.

By withdrawing his or hers consent, the user is ensured that their personal data will not be used in future customer satisfaction surveys.



We can see from the figure 3.6 that we have one activity called “Block opinion-research institutes”, which we have not talked about earlier. This activity is basically a switch.

It has itself as condition, which means it cannot be executed. “Send data to opinion research institutes” has “Block opinion research institutes” as condition, and since it cannot be executed the only way to execute the send activity is to exclude the block activity. This can only be done by executing “Give consent”. If the data subject wants to withdraw his consent, it will include “Block opinion research institutes” again, and thus “send data” will not be executable.

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

***Data protection by design and default :*** The protection of personal data has to be as much as possible designed into the system, and turned on by default, and not left to the user to activate. It includes many different concepts such as data minimization, data pseudonymization and encryption .

***Data minimization :*** Is a concept stating that the company should not process more informations that it actually needs to achieve the purpose for which the data was given by the data subject.

***Data pseudonymization :*** the regulation defines it as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.” it is thus the process of separation of data from direct identifiers, which would be kept separately. It helps reducing the risk for the data subject.

***Data anonymization :*** making the set of data in such way that no individual can be identified by any way, either by encrypting or removing personal identifiers.

***Appoint a DPO :*** appointing a data protection officer is not a legal obligation in every case. Data protection officers must be appointed for public authorities and companies where the main activity involve “regular and systematic monitoring of data subjects on a large scale” or processing of large data sets containing special categories of personal data such as ethnicity, religious or philosophical beliefs, also called sensitive personal data. It is however a good practise to appoint a person who is responsible for assessing the company’s processing of personal data

***IT-supplier :*** the it supplier is a company that is responsible of maintaining the system

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

[y] p.54 <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

[z] <http://www.out-law.com/en/articles/2016/may/gdpr-potential-fines-for-data-security-breaches-more-severe-for-data-controllers-than-processors-says-expert/>

[t] <https://en.wikipedia.org/wiki/Pseudonymization>