1 Introduction

The focus of this essay is on changes proposed in the European Data Protection Regulation (EDPR) by the European Commission. A summary of changes proposed will be presented and a discussion of amendments made to the to the regulation made in October 2013.

Additionally, a discussion of the regulation's conversy will be presented. Public bodies and companies have raised questions about the regulation and a therese is a growing a controversy about the effect the regulation on business and the bureaucracy level.

Furthermore, changes to the computing professional practice relevant to the regulation will be examined and main points required to ensure compliance will be presented.

2 European Data Protection Regulation

The EDPR is a framework proposed by the European Commision (EC) in January 2012 as a way to replace current regulations in the European Union. According to the EC, the aim of the framework is to "*modernise, simplify and strengthen the data protection framework, in order to unlock the full potential of the single market*" (European Commision, 2013). The main purpose for such a radical change is, according to the European Commision, 2013, "fragmentation of rules between EU countries".

Firstly, the regulation aims to provide common legal ground for all European countries. The regulation defines the creation of single Data Protection Authority responsible for the approval and monitoring of rules for businesses regarding data. Additionally, the authority would be responsible for deciding pecuniary penalty. Requirement for a separate authority in each member country would be eliminated. Companies would no longer be required to conform to varying requirements, reducing their expenses. This in turn would be enforced on the company level for companies with more than two hundred and fifty employees by a Data Protection Officer responsible for the correct practice maintained within the company.

Secondly, European Commision claims that personal data is a "fundamental right for everyone in the EU and must be safeguarded" (European Commision, 2013). This leads to a decision for companies collecting information from users to require explicit consent to store user data on the server. Additionally, consent cannot be required to complete a registration unless the data required is necessary for the service's core functions. Conversely, a user shall have a

”qualified 'right to be forgotten'; giving individuals a general right to force organisations to delete personal data stored about them ‘without delay’” (Out-Law.com, 2013). Alternatively, the user should have the option to send their data directly to a different service provider and upon request, the service provider should provide the user with data they hold about them - for a reasonable charge.

Thirdly, the issue of data breach and unlawful access to date is changed. Data holders - companies and public bodies - would be required to notify the Data Protection Agency of any such events within twenty four hours of discovery of the incident. The Data Protection Agency then takes specific steps in order to ensure the scope of the damage is mitigated. Additionally, this is further enforced by the regulation as having “‘privacy by design’ and ‘privacy by default’” (European Commision, 2013), ensuring sufficient procedures are in place to prevent data breach rather than attempt to mitigate the impact.

Amendments to the Data Protection Regulation were made on 21st October 2013 and included the following changes, according to TwoBirds.com, 2013. Fines have been increased up to one hundred million euros or five percent of annual worldwide turnover. Data subjects should be provided the right to know if the personal data has been disclosed to a public authority - inspired by recent developments regarding the US based PRISM surveillance project. Additionally, companies will be required to gain consent from the Data Regulation Authority if they wish to process more than 5000 data subjects in a consecutive 12 month period. Furthermore, the leading supervisory activity will be required to consult other regulatory bodies in order to make an informed and balanced decision in the case of a breach of the Data Protection Regulation.

3 Controversy

Despite the overwhelming claims of future improvements and less red tape made by the European Commision, there are issues that companies, particularly start-ups, are not comfortable with. It is claimed by Peter Schar that “there is a real need for an international regulatory framework. For once, the Americans are as concerned about this as we are in Germany" (The Guardian - Britain EU Data Protection Law, 2013). However, issues have been raised where the requirement for data consent will hurt start up businesses. The Drum, 2013, states “The result would be a more ‘logged in’ digital environment, reducing the business incentive to

invest or build in security or privacy measures and without necessarily affording additional safeguards for consumers." The argument put forward is the following, with increased required consent for internet advertising, financing a startup through advertising will become very difficult and may lead to a decreased incentive for entrepreneurs to sacrifice their opportunity cost. This argument is further described as "too prescriptive in terms of its administrative detail and said it would therefore end with already suffering small- and medium-businesses -- which the UK government has repeatedly said will be core to economic recovery -- taking the brunt of the burden." (Wired.co.uk - ICO Commisioner slams.., 2013), this is especially true in the case the UK which strives to reduce 'red tape' for small and medium sized businesses as an incentive to to economic growth.

Conversely, "if a third country requests a company (eg. a search engine, social network or cloud provider) to disclose personal information processed in the EU, the firm would have to seek authorisation from the national data protection authority before transferring any data" (The Next Web, 2013). Such requirements would, however, cause large companies such as Google and Facebook facing fines, unless changes are made, since their server base is outside of the European Union. This presents a an issue for both the users and the corporations. <TODO>

Moreover, the creation of a European Union wide regulatory body may reduce citizens ability to interact with the body due to a distance and language barrier. It is claimed that only about a third of european citizens have any knowledge of the existence of a national public authority tasked with protection of their personal data (European Commision Documents, 2013). One cannot but wonder if the introduction of a European Wide Regulatory body will increase awareness. The European Commission claims in its Documents that it will indeed do so, however, the issue of awareness does not address the ability of citizens to access the regulatory body in a simple and bureaucratic-less manner.

Furthermore, it is argued by the European Commision that a greater control over data is required European Union wide, however, Germany already has a data protection law which requires a data protection officer to be hired for each company with at least nine employees (Judy Schmitt, Florian Stahl, 2013) - this is considerably less than what the European Commision is proposing. The result would be less regulation for some European countries may be deemed undesirable by the German government.

Finally, contradictory to the European Commission's claim for clearer and less broad data protection law, “a majority of companies in the UK do not have a clear grasp of how data protection regulation will change once the EC proposals are enforced. Moreover, this lack of understanding persists for companies that hold over 100,000 records of personal data, and presumably dedicate a significant amount of resources to data collection, processing and storage” (ICO.uk.org, 2013). This would suggest that the regulation itself is not so clear cut and may in fact be fairly complicated to understand and implement by companies. Additionally, this may lead to varying interpretations and yet again fragmented regulation practice.

4 Computing professional guidance

Firstly, all computing professionals should “ensure that [they] have the knowledge and understanding of legislation and that [they] comply with such legislation, in carrying out [their] professional responsibilities” *(BSC.org,2013)*. Particularly, understanding the scope of the legislation and the effect one’s computing practice will have. This is especially relevant if the product or service will be used inside the European Union as well as elsewhere.

Secondly, ensure that standards of the professional practice are maintained. Additionally, make effort to implement solutions for data loss prevention are minimized through precautionary measures and ensure any known data loss or security breach is announced to the Regulation Authority within twenty four hours. This goes in hand with the guidance given on BSC.org. Furthermore, do “NOT disclose or authorise to be disclosed, or use for personal gain or to benefit a third party, confidential information except with the permission of your Relevant Authority, or as required by Legislation” *(BSC.org,2013)*, in respect to the Data Protection Legislation, computing professionals should ensure trade and move of data is not carried unless consent from the regulation body is given.

Thirdly, responsibility for potential Data Protection Legislation breach should be taken immediately by the professional and all information leading to the incident should be disclosed to the relevant authority in order to mitigate the impact as described in the computing professional code of conduct. Clients should be informed of the breach and sufficient precautionary measures should be taken to prevent future incidents.

5 Conclusion

The data protection reform crafted by the European Commision aims to put the client in control of their data and aims to update the European legislation with technological advancement of the internet age in mind. Privacy of individuals is claimed to increase as trade with data and personal information is to be monitored. Conversy over the legislation arise as member countries attempt to push for modifications or oppose the legislation altogether. There is a rising concern over the impact on small business and their ability to surivive in the market while having to comply to the regulation. Larger business fear loss of ‘free’ trade with data and changes to their business strategy. Either way, current laws are not up to date with the reality and will require changes to stay up to date and provide a relevant ground for businesses to follow.

References:

- **European Commision Documents - Factsheets on data protection reform, 2013**.
  [Web Resource] *http://ec.europa.eu/justice/data-protection/document/index_en.htm*
  [Visited November 8, 2013]
- **Out-Law.com - UK seeks opt-out of "unrealistic" European 'right to be forgotten' laws, 2013.**
  [Web Resource] *http://www.out-law.com/en/articles/2013/april*
  /uk-seeks-opt-out-of-unrealistic-european-right-to-be-forgotten-laws/
  [Visited November 8, 2013]

- **Bird & Bird - EU Data Protection Regulation: one step forward**
  [Web Resource] *http://www.twobirds.com/en/news/articles/2013/global/libe-committee*
  -of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft
  [Visited November 8, 2013]
- **The Guardian - Britain EU Data Protection Law**
  [Web Resource] *http://www.theguardian.com/technology/2013/sep/27/britain-eu-data-protection-law*
  [Visited November 8, 2013]
- **Judy Schmitt, Florian Stahl - How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide**
  [PDF] *https://www.privacyassociation.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf*
  [Visited November 8, 2013]
- **ICO.org.uk - Implications of the European Commission's proposal for a general…**
  [PDF] *http://www.ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports*
  /implications-european-commissions-proposal-general-data-protection-regulation-for-business.ashx
  [Visited November 8, 2013]
- **Wired.co.uk - ICO Commissioner slams EU data protection directive**
  [Web resource] *http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection*
  [Visited November 16, 2013]
- **The Next Web - Facebook, Google and others could face fines of €100m if they break proposed data protection rules**
  [Web Resource] *http://thenextweb.com/eu/2013/10/22*
  /facebook-google-others-face-fines-e100m-break-proposed-data-protection-rules/
  [Visited November 16, 2013]
- **BSC Code of Conduct**
  [Web Resource] *http://www.bcs.org/category/6030*
  [Visited November 16, 2013]