Legal frameworks eea and global entrepreneurship law company business partnership...

Law

INTRODUCTION

Due to the expansion of the Internet's use by individuals globally and the rapid growth of the Internet itself in the early 90's, it was inevitable that massive collections of user data were being transferred and stored in computers across countries and continents as a means to carry out secure transactions, user identifications, discussions between users and exchanges of ideas and various other client-server affairs or interactions between users. The nature and sensitivity of such data could vary from articles and posts containing thoughts, beliefs and ideas or expressions of opinion to more important personal data such as credit card details and telephone numbers. In any case, it has been a common practice amongst users (living individuals) to send data to be stored at servers worldwide, from which they can be identified or even be affected in real life in cases of misuse by the data holders. It's also a reality, as the organization of the public and private

sector’s services gets more and more computerized, that governmental bodies or private companies can hold offline databases filled with the data of citizens who either deliberately use their services or compulsory as subjects to the law, and in such cases there’s usually more sensitive personal data involved such as physical or mental health, economic data and home addresses. Moreover, apart from give-take data scenarios, personal data has always been vulnerable to misuse by third parties as it ‘ travels’ across networks or within the network of the data subject. All this gave rise to a variety of new computer issues with impact to lives of real people. Questions arisen, as – for instance - what rights do data holders have over the users’ personal and sensitive data and in what ways are they permitted to process it. Thus, there was a need for regulation and laws over user data that would protect the user and his rights on his personal information, a legal framework that would give rights to data subjects and place obligations on data controllers.

EU/UK legislation for personal data protection

In Europe, the Data Protection Directive (D. P. D.) was introduced in October 24th 1995 to regulate the processing and free movement of personal data within the European Union (Official Website of European Union, n. d.). It incorporated seven principles, previously issued as guidelines by the Organization for Economic Cooperation and Development (OECD) in 1980 (Wikipedia #1, n. d.). Those were: Notice—data subjects should be given notice when their data is being collected; Purpose—data should only be used for the purpose stated and not for any other purposes; Consent—data should not be disclosed without the data subject’s consent; Security—collected data

should be kept secure from any potential abuses; Disclosure—data subjects should be informed as to who is collecting their data; Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; andAccountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles. The DPD outlines that Personal data should not be processed at all, except when certain conditions are met and it regulates the processing of personal data regardless of whether such processing is automated or not. Worth mentioning that, above all, the data subject has the right to be informed when his personal data is being processed and data may be processed only when the data subject has given his consent. In 1998, a few years later, a UK law on the processing of data was introduced to bring the United Kingdom into line with the DPD. The Data Protection Act (D. P. A.) of 1998 replaced and consolidated earlier legislation such as the Data Protection Act 1984 and the Access to Personal Files Act 1987 and it aimed to implement the European DPD (Wikipedia #2, n. d.). The Act defines eight data protection principles:(From IST students stfs public folder, PIC module, " Data Protection & the DPA")Personal data shall be processed fairly and lawfully. Personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed. Personal data shall be accurate, and where necessary, kept up to date. Personal data shall not be kept for longer than is necessary for the purposes for which it is being processed. Personal data shall be processed in accordance with the rights of

data subjects under this Act. Appropriate security measures shall be taken against the unauthorized or unlawful processing, accidental loss, destruction, or damage of personal data. Personal data shall not be transferred outside the EEA unless that country / territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Under DPA a data subject can make sure his personal data is not misused, get it put right if it’s wrong and even have it deleted if it’s no longer needed, thus the Act puts emphasis on how important it is to know what is held about us as individuals in order to apply all the above.

EU/UK legislation and contemporary entrepreneurship in EEA

The DPD and DPA shaped the way that data is being processed nowadays within the European Economic Area (EEA) and the way it gets transferred across networks and countries in and out of it. Every data holder that handles personal data of individuals is obliged under the DPA to inform the Information Commissioner’s Office (ICO) that enforces data protection and deals with DPA matters as well as investigates breaches of the Act. Personal data must not be processed unless the data holder has been licensed by the Commissioner, according to DPA 1988, Chapter 3, section 17 (Official UK legislation Website, n. d.). Additionally, apart from being included in the register maintained by the Commissioner prior to processing, it is required to annually renew the license. Moreover, the processing and maintenance of the data must comply with the aforementioned principles defined by the Act. Data holders have to consider a number of obligations and avoid any

violation of the Act by taking the appropriate measures. To mention some, they have to secure the data against unauthorized or unlawful access and processing, accidental loss, destruction or damage and be able to present the data in a relevant filing system when needed, which means that the system’s storage should be implemented in a way that specific information that is related to a particular individual can be accessible when required. Modern businesses within the EEA have been greatly affected structurally and economically in the process of complying with the European legislation. They often require additional manpower that expertizes on certain tasks and additional software. They have to carry out all the appropriate measures to: 1. Be in line with it. Thus, there’s demand for systems designed to protect data from unauthorized access and create backups to prevent data loss. As a result, there is also great demand for software developers who can create systems that can efficiently process and protect data. 2. Avoid breaching it. Thus, there’s demand for attorneys and lawyers for legal advice and assistance in case of legal matters. Furthermore, businesses turn to legal assistance in cases of gray areas of the Act and whereas they need to lawfully transfer the data within EEA or out of it or even to bypass their legal obligations. 3. Bypass their legal obligations. Pressure to reduce costs by outsourcing development and processing to countries where there is no DPA.

Legal frameworks outside EEA and global entrepreneurship

The United States uses a 'sectoral' approach to data protection legislation, relying on a combination of regulation, self-regulation and legislation, rather than governmental regulation alone. To date, the US has no single data protection law comparable to the EU's Data Protection Directive. Privacy

legislation in the United States tends to be adopted on an ad hoc basis, with legislation arising when certain sectors and circumstances require it (e. g., the Video Privacy Protection Act of 1988, the Cable Television Protection and Competition Act of 1992, the Fair Credit Reporting Act, and the 2010 Massachusetts Data Privacy Regulations). Therefore, while certain sectors may already satisfy the EU Directive, at least in part, most do not. Canada is one of the countries closest to the European Union in terms of comprehensive information privacy law. It uses a coregulatory framework between the government and the privacy sector to enforce data protection. The Privacy Act of 1983 regulates the use of personal information by the Canadian Federal Government. It requires that the data subject is made fully aware of the information collected and its uses, that he provides explicit consent before information is disclosed to parties outside the control of a government institution (with a few exceptions) and that he has the right to access personal information held by a government institution and rectify erroneous information. The enforcement of the Act is controlled by the Privacy Commissioner of Canada is a special ombudsman and an officer of parliament who reports directly to the House of Commons and the Senate and like the European Commissioner he has the authority to investigate complaints filed by Canadian citizens, and report on whether there has been a violation of the Privacy Act (Wikipedia #3). Across Asia Data Protection is varied depending on the development and political beliefs of each country, however even counties that grant the least amount of protection have shown a concern for Data Protection and the way it affects the free flow of information. For instance, in Japan the Personal Information Protection Act

was introduced in 2003 and became fully effective on 1/4/2005 (CIPP Guide Website). Due to the various different legal frameworks and/or legislations worldwide, entrepreneurship is affected on a global scale as there are different rules that apply in exporting data in different countries. As a result of these differences, the ability of U. S. organizations to engage in a range of trans-Atlantic transactions could have been significantly hampered by the Directive. The European DPD prohibits the transfer of personal data to non-European Union countries that do not meet the European Union (EU) " adequacy" standard for privacy protection and the EU Member States require that their residents’ personal information not be transferred to countries that do not protect that information adequately. In 2000, the EU ruled that the United States (US), through its voluntary Safe Harbor program, met that requirement. The Safe Harbor scheme (not a law) sets out a framework of data protection standards which allow the free flow of personal data from EEA data controllers to the US organizations which have joined the scheme. In order to be eligible to join the Safe Harbor scheme, a US organization must be monitored or regulated by an independent statutory body which can protect personal privacy effectively and has jurisdiction to investigate complaints. The Federal Trade Commission ('FTC') and the Department of Transportation ('DOT') are such statutory bodies recognized by the European Commission (IST College, " The US Safe Harbor Scheme"). http://export. gov/safeharbor/eu/eg_main_018476. asphttps://www. cippguide. org/2009/12/06/data-protection-laws-around-the-globe/http://www. international. gc. ca/apec/map-carte. aspx? view= d

Conclusion:

Although legislation for the protection of personal data exists on a global scale, there is still much progress to be done in order to effectively protect it since in most places of the world there is still inadequate legislation, if any at all. And since the Internet has no boundaries in regard to where the data flows, inadequacies in one country’s legislation can affect the effectiveness of legislation in other countries. For instance, a European resident can outsource development and processing to India or to another country where there is no DPA and still achieve any processing or marketing that has been forbidden to his business which operates within the EEA. And although that requires additional effort for the average businessman, the DPD and DPA are deemed utterly useless.