THE DATA PROTECTION LAW OF IRELAND AND EUROPEAN UNION

By
Aaditya Dharma Sivasubramanian
19155930

MSc Cyber Security

Lecturer: Irene Fisher, B.L

National College of Ireland

Dublin

Introduction

Under GDPR, a photograph is treated as vital personal data. Primarily a photo sharing website gathers and stores customer images. In Ireland, businesses must abide by the General Data Protection Regulation (EU) and the Data Protection Act (Ireland). Organizations must ensure that consumer data is secure and that their security systems are essential. This report will discuss the data protection regulations in the European Union and Ireland in detail and will outline ways of complying with the rules on the processing of customer personal data.

Personal Data protection

The European Parliament adopted General Data Protection Regulation (EU) 2016/679 for the protection of individuals with respect to the collection of personal data and the free flow of such data, repealing Directive 95/46/EC (General Data Protection Regulation), which took effect in all 28 European Union (EU) countries on 25 May 2018.
As a Public oversight, the GDPR does not generally require transposition into Irish law, as EU Regulations have “direct effect”.

Ireland adopted legislation known as the Data Protection Act 2018 that was signed into law on 24 May 2018. The new Act, along with the previous data protection laws, will be collectively known as the ' Data Protection Acts 1988-2018, ' intended to protect the privacy of individuals. The legislation confers rights on persons with respect to the protection of their personal data as well as obligations on those who keep and process these data.

When a company has traffic from a European country, the GDPR refers to the protection of the data that our website gathers regardless of where we are headquartered, where the website is hosted, where the client is located. GDPR does protect Personally Identifiable Information (PII) including: Name, address and ID numbers, location, IP address, cookie data and RFID tags, health and genetic data, Biometric data, Racial or ethnic data, Political opinions and sexual orientation. Businesses shall be allowed to store and process personal data from the EU only if they agree to it individually and for "no longer than is appropriate for the purposes for which personal data are stored." This ensures that, personal data must also be portable from one organization to another, and on request, business must remove personal data. Additionally, the organization will ensure that every agency collects or stores data for us is following the GDPR. The GDPR holds processors liable for any breach or failure to comply. It is possible that our company as well as our processing partner such as cloud provider will be liable for penalties even if the fault lies entirely with the processing partner or data storage. This could include website host, email host, cloud, Software as Service applications and other computer programs we use in our business.

The organization need to examine how the merchants oversee and make sure about information from EU based exchanges to comprehend the dangers they present. The agreement between the organization and the merchant need to characterize predictable procedures for how information is overseen and secured, how ruptures are accounted for. The 72-hour detailing window that the GDPR requires makes it particularly significant that merchants realize how to appropriately report an individual information rupture to the business. The GDPR subtleties punishments of up to €20 million or 4 percent of worldwide yearly turnover, which is higher, for rebelliousness. On the off chance that there is close to home information rupture, the GDPR necessitates that organization report individual information breaks inside 72 hours to the supervisory authority of the nation in which the EU residents influenced by the rupture live. How well business limit the harm will legitimately influence the organization's danger of fines for the rupture.

Processing of Personal data (Article 5)

1. Lawfulness, fairness and transparency
   Personal data must be processed lawfully, fairly and in transparent manner in relation to the data subject.
2. Purpose Limitation
   Individual information gathered for determined, unequivocal and real reasons for existing are not additionally handled in a way that is incongruent with those reason, further preparing for filing purposes in the open intrigue, logical or verifiable research purposes or measurable purposes will, as per Article 89(1), not to be viewed as inconsistent with the underlying purposes.
3. Data Minimisation
   Adequate, relevant and limited personal data must be collected, to what is necessary in relation to the purposes for which they are processed.
4. Accuracy
   Personal data must be accurate and, where necessary, kept up to data. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay.
5. Storage Limitation
   Individual information kept in a structure which grants distinguishing pieces of proof of information subjects for no longer than is essential for the reasons for which the individual information is handled. Individual information might be put away for longer periods to the extent that the individual information will be forms exclusively for filing purposes in the open intrigue, logical or recorded research purposes or factual purposes as per Article 89(1). Subject to execution of the suitable specialized and authoritative estimates required by this guideline to defend the rights and opportunities of the information subject.
6. Integrity and Confidentiality
   Personal data 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.

Case study:

In 2019, President of Personal Data Protection Office (PDPO) found that the company ClickQuickNow Sp. Z o.o. did not implement appropriate technical and organizational measures that would enable easy and effective withdrawal of consent to the processing of personal data and the exercise of the right to obtain the erasure of personal data (“The right to be forgotten”). Thus, it violated the principles of lawfulness, fairness and transparency of processing of personal data, and inconsistent with Article 7(3) specified in GDPR. The PDPO imposed an administrative fine of EUR 44000.

Data Protection Officer (DPO)

The essential job of Data Protection Officer (DPO) is to guarantee that the association forms its individual information staffs, clients, suppliers or some other people (information subjects) in consistence with the relevant information security rules. In the EU foundations and bodies, the Article 37 of Data Protection (Regulation (EU) 2018/1725) obliges them each to designate a DPO. Guideline (EU)2016/679, which obliges a few associations in EU nations to delegate a DPO.

The DPO is an indispensable piece of the association, making him/her undeniably put to guarantee consistence. In any case, the DPO ought to have the option to play out his/her obligations autonomously. IN EU organizations and bodies, there are a few confirmations ensuring this freedom.

1. The applicable rules of EU institutions and bodies expressly provide that the DPO Shall not receive any instructions regarding the performance of duties.
2. There must not be a conflict of interest between the duties of the individual as DPO and his/her other duties, if any. To avoid conflicts, it is recommended that
    - A DPO should not also be a controller of processing activities
    - The DPO should not be an employee on a short or fixed term contract
    - A DPO should not report to a direct superior (rather than top management)
    - A DPO should have responsibility of managing his/her own budget
3. The Organisation must offer staff and resources to support the DPO to carry out his/her duties. In this respect, DPOs in EU institutions and bodies can be seconded by a assistant or deputy DPO, and can rely on data protection coordinators (DPCs) in each section of the organization. Access to resources also includes training facilities.
4. The DPO should have the authority to investigate. In EU institutions and bodies, for instance, DPOs have immediate access to all personal data and data processing operations. Those in charge are also required to provide information in reply to his/her questions.
5. A minimum term of appointment and strict conditions for dismissal must be set out by the organization for a DPO post. In the EU institutions and bodies, the DPO is appointed for a period between 2 and 5 years, may be reappointed for up to a maximum of 10 years and can be dismissed only with the consent of the EDPS.

Roles and Responsibilities of DPO

The DPO has to ensure that the data protection rules are respected in cooperation with the data protection authority (for the EU institutions and bodies, this is the EDPS). The DPO must abide to the GDPR regulations as elaborated in Article 39 In the EU institution and bodies, the DPO must:

- Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;
- Give advice and recommendations to the institution about the interpretation or application of the data protection rules;
- Create a register of processing operations within the institution and notify the EDPS those that present specific risks (so-called prior checks)
- Ensure data protection compliance within his/her institution and help the latter to be accountable in this respect.
- Handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative.
- Cooperate with the EDPS (responding to his requests about investigations, complaint handling, inspections conducted by the EDPS, etc.)
- Draw the institution's attention to any failure to comply with the applicable data protection rules.

Case Study:

In 2019, The Federal Commissioner for Data Protection imposed a GDPR fine of EUR 10,000 on Rapidata GmbH because the company had not appointed a Data Protection Officer (DPO). The company failed to comply with its legal obligation under Article 37 GDPR to

appoint a company data protection officer. Since the company was in the category of micro-enterprises, fine of EUR 10000 was imposed on 9th December 2019.

Data Processing Agreement

The GDPR necessitates that an agreement be set up between an information controller and any information processors the controller employments. Practically every business depends on outsiders to process individual information. Regardless of whether it is an email customer, a distributed storage administration, or site examination programming, a Data Processing Agreement fulfills this prerequisite with every one of these administrations to accomplish GDPR consistence. The EU GDPR adopts more genuine strategy to contracts than past EU information guidelines did. Ever association that is dependent upon the GDPR must have a composed information preparing understanding set up with any gatherings that go about as information processors to conform to GDPR and to evade GDPR fines.

Data Controller is the characteristic or lawful individual, open power, organization or other body which, alone or mutually with others, decides the reasons and methods for the handling of individual information. Where the reasons and methods for such handling are dictated by Union or Member State law, the controller or the criteria for its selection might be accommodated by Union or Member State law.

Data Processor is a characteristic or lawful individual, open position, office or other body which forms individual information for the benefit of the information controller.

Information handling understanding (GDPR Article 28, Section 3) must cover following focuses in it

- The processor agrees to process personal data only on written instructions of the controller
- Everyone who comes into contract with the data is sworn to confidentiality.
- All appropriate technical and organizational measure are sued to protect the security of the data.
- The processor will not subcontract to another processor unless instructed to do so in writing by the controller, in which case another DPA will need to be signed with the sub-processor (pursuant to Section 2 and 4 of Article 28).
- The processor will help the controller uphold our obligations under the GDPR, particularly concerning data subject's rights
- The processor will help the controller maintain GDPR compliance about Article 32 (security of processing) and Article 36 (consulting with the data protection authority before undertaking high-risk processing).
- The processor agrees to delete all personal data upon the termination of services or return the data to the controller.
- The processor must aloe the controller to conduct an audit and will provide whatever information necessary to prove compliance.

Since the GDPR went into power, information assurance specialists have exhibited their readiness to give punishments. Also, little and medium-sized organizations were not disregarded. Be that as it may, there are two feels burnt out on fines, contingent upon the seriousness and kind of infringement. GAPR fines gave for infringement identified with information processors commonly fall under the primary level, which rules state can be serious as € 10 million or 2% of worldwide income. Regardless, it is substantially less difficult to consent to an information preparing arrangement and stick to the terms than it is pay a GDPR fine.

Case Study:

In 2018, the Tennis Association KNTLB sold personal data of a few hundred thousand of its members to two sponsors without legal basis. The following data categories were sold to sponsors by The Royal Dutch Lawn Tennis Association (KNLTB): name, gender, photograph and address. The aim was that the sponsors would be able to approach the data subjects and make them tennis-related and other offers. For any processing of personal data, the Controller must be able to reply on one of the six legal bases for processing in Article 6 GDPR. In the view of the DPA the sale of personal data without the consent of the data subject concerned is generally prohibited (Article 6). The Tennis Association was fined EUR 525k for selling the data on 3rd March 2020.

GDPR and Photographs handling

Personal Identifiable Information (PII) is any data identifying with a recognizable individual who can be straightforwardly or in a roundabout way distinguished by reference to and identifier. This gives wide scope of individual identifiers to establish individual information, including name, distinguishing proof number, area information or online identifier, reflecting changes in innovation and the way associations gather data about individuals. Photos contain biometric data for the face and that makes them touchy information and along these lines, they are close to home information under GDPR. PII must be agreed to except if the photo is utilized for purposes like news or workmanship.

Data controller needs unequivocal agree to store, process or distribute except if the photo is for work or government ordered purposes. EU inhabitant individual must be educated regarding their date security rights under GDPR including the option to get to, to one side to eradication, the privilege to information movability and the option to pull back assent. For more seasoned photos, if the organization had authoritative assent for the sharing of a picture of one of its subjects at the hour of accommodation of photo, at that point the laws at the hour of accommodation apply with certain admonitions. Under GDPR if the subject of the photo pulls back agree for to process, store or distribute that picture, the organization may should have the option to evacuate them. Notwithstanding, this would be pending an agreement in which the subject consented to permit this, and which would then not license them to pull back assent or require the organization to expel or eradicate the pictures. It is a decent broad business practice to have a reasonable information and report maintenance strategy and to hold fast to it. It is required to get the assent of a gatekeeper for minors (younger than 18) to utilize their photos.

On the off chance that a picture of an individual with no name, work, age, area data or anything interestingly recognizable data is ruptured, at that point the lawful rights and opportunities of the picture subject is probably going to viewed as negligible. In an alternate situation, if the electronic client connection the executives programming (CRM) is connected to organization's online photograph displays for explicit customers, that it contains name, address, duplicates of agreements and marked waivers connected to those pictures and the entirety of this is broken. This could significantly affect the protection rights and opportunities of the people in question.

Conclusion:

GDPR give people broad rights over their information and present exacting principles over how organizations gain, store and utilize that information. The expense of resistance is very high in both monetary and nonfinancial terms, making the choice of doing nothing because of GDPR invalid. While "General" shows up in the title of the GDPR connoting a recently orchestrated and bound together way to deal with information insurance to be applied across Europe. The "G" could similarly mean "Worldwide". The guidelines apply to each association

anyplace on the planet that controls or procedure individual information of EU occupants, and budgetary punishments system for associations found in rebelliousness in dependent on complete overall income, not just on income earned inside EU part states. Compliance to the laws and regulations are the best practice in interest of both the company and the customers.

References:

[1] General Data Protection Regulation (GDPR). (2016). General Data Protection Regulation (GDPR). [online] Available at: https://gdpr-info.eu/ [Accessed 17 Mar. 2020].
[2] General Data Protection Regulation (GDPR). (n.d.). Data Protection Officer. [online] Available at: https://gdpr-info.eu/issues/data-protection-officer/ [Accessed 17 Mar. 2020].
[3] Data Protection Legislation | Data Protection Commission. (2018). Data Protection Legislation | Data Protection Commission. [online] Available at: https://www.dataprotection.ie/en/legal/data-protection-legislation [Accessed 17 Mar. 2020].
[4] Europa.eu. (2016). EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504 [Accessed 17 Mar. 2020].
[5] www.nathantrust.com. (n.d.). GDPR Fines and Penalties. [online] Available at: https://www.nathantrust.com/gdpr-fines-penalties [Accessed 20 Mar. 2020].