**What is General Data Protection Regulation (GDPR)?**

General Data Protection Regulation (GDPR), a regulation drafted and passed by the European Union (EU) that lays down rules of the protection of natural person with regard to the processing of personal data and rules relating to the free movement of personal data, it protects fundamental right and freedoms of natural person and in particular their rights to the protection of personal data.

Data protection principles given by (Your Europe, 2022)

∙ Lawfulness, fairness and transparency — Processing must be lawful, fair, and transparent to the data subject.

∙ Purpose limitation — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

∙ Data minimization — You should collect and process only as much data as absolutely necessary for the purposes specified.

∙ Accuracy — You must keep personal data accurate and up to date.

∙ Storage limitation — You may only store personally identifying data for as long as necessary for the specified purpose.

∙ Integrity and confidentiality — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality.

∙ Accountability — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

**How does it work?**

The GDPR is applied under two circumstances, the first one is the organization processes personal data and is based in EU, no matter where the actual data processing takes place. The second one is the company is established outside EU but dealing with personal information in relation to the offering of goods or service to the individuals in the EU. Since financial intelligence units need personal information to trace

Financial intelligence units are operationally independent autonomous entities established in all EU Member States and are tasked with receiving (and, as permitted, requesting), analysing, and disseminating financial information, including personal data, via STRs ().

They play an important role in detecting the money laundering and funds that is used for terrorism. Based on the working principles of them, they are positioned between the private sector and LEAs. In other words, FIUs serve as the inter. acting as intermediaries, serve as the central reception point for receiving financial disclosures64 from obliged entities.65 Where, after the FIU analyses the material, there is a suspicion of money laundering or terrorist financing, the FIU shall forward the result of its analysis to the national authority responsible for prosecution (Teresa,2022). Therefore, financial intelligences are required to follow the instructions and monitoring of GDPR. To meet the requirement of complying with the GDPR, financial intelligence unit has formed a GDPR working group which includes representatives from the Office of the General Counsel, the Office of University Compliance and Integrity, and the Division of Information Technology (FIU Compliance Office, 2019). However, GDPR provides on a general solution on dealing with individuals data and is able to be considered as general limitation clause and does not explicitly distinguish them from other competent authorities.

**What Information Is Collected by FIUs**

∙ Contact information – home and business addresses, phone numbers, email addresses, and social media contact information

∙ Demographic information – names, titles, gender, birth and death dates, and ethnicity

∙ Student information obtained from campus records – degrees, majors, organization involvement, activities, awards, and sports involvement

∙ Employment information – company names, job titles, and industry information

∙ Family information – spouse’s name, children’s names and birth dates, and familial relationships

∙ Alumni information – activity interest and participation, event attendance, volunteer interests, organization affiliations, committee participation, awards and honors, attitudes and preferences

∙ Donor information – giving information regarding any donation which is made or for which someone receives credit

∙ Analytical information – aggregated transactional information related to web visitor activity and email marketing action

**Issues when addressing the requirements of GDPR**

For the aim of gathering information that serve for forensic of money laundering and terrorism, financial often needs to request information from their counterparts in the other EU member states. This leads to a issue that each financial intelligence units does not allow a specific structure and different models have developed based on various function and national status. For instance, a few nations follow the instructions of General Data Protection Regulation, while some others comply with the Police Data Directive. This may lead to problems as some process of data may be acceptable

Therefore, a common law enforcement implemented in all member states is necessary and this is why FIU must follow the instruction of General Data Protection Regulation. However, another issue appear as financial intelligence require to process personal data in order to track economic crimes, it will be much more difficult for FIUs to conduct their investigation on money laundering and terrorism if they are more restricted by GDPR.

Quintel (2022) also stated that although the GDPR is based on strong transparency obligations towards data subject, its system on the restriction of data subject rights lacks such specific provisions that would compel controllers to inform data subjects after a restriction has taken place, which means that data subjects will not be informed about whether restriction prevent their personal information being used or not. Refer to the financial intelligence unit cases, it would be good news since the data subject may be a criminal that suspect of committing money laundering or provide financial support for terrorism.

**Conclusion**

In general, complying with General Data Protection Regulations is essential for financial intelligence units in spite of the difficulties that it will bring. FIUs should consider the conservation of personal information and make sure the personal information is safe and not be misused by any unauthorized third parties. On the other hand, since various FIU counterparts located in different EU members, their privacy regulation vary and need to be unified in the near feature to avoid the inconsistency of transferring data between one FIU to another.

Reference

Quintel, T. (2022). Data protection rules applicable to Financial Intelligence Units: still no clarity in sight. *ERA Forum: Journal of the Academy of European Law*, *23*(1), 53–74. <https://doi.org/10.1007/s12027-021-00697-z>

Data protection under GDPR - Your Europe. (2022, June 7). Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index\_en.htm#:~:text=The%20GDPR%20sets%20out%20detailed,people%20living%20in%20the%20EU.

Collection of Information - FIU Compliance Office. (2019, December 18). FIU Compliance Office. https://compliance.fiu.edu/privacy/collection-of-information/