**Computer Security for Developers**

**Why are Companies Legally obliged to protect their systems?**

Companies are obliged to legally protect their system to guarantee the protection of personal data whenever they are collected and appropriate use of data at the owner’s consent.

Regardless of the format a data takes, whenever this is directly or indirectly identifying individual data is stored or processed, the data protection right is invoked and must protect. The European Union General Data Protection (GDPR) describes the different occasions whereby an organization can collect or reuse personal information with the intention of protecting and be responsible for it.

So, when Is Data processing or Storage is allowed?

* Whenever an organization or a company has a contract with an individual to supply goods or services.
* When an individual is complying with a legal obligation for legal requirements such as monthly payments, subscription, social security etc.
* For public task or academic involvement in relation to public administration, for example, registration for school, hospitals and municipal involvements.
* When a legitimate interest is involved such as bank registration, or civil registration etc.

For these to be valid the organization or company ask individuals for their consent to use their data.

Every data owner has the right to terminate their agreement to the use of their Data. Even after consenting your right to withdraw remains valid for as long as one wants it, once the permission has been withdrawn, the organization no longer has the right to the Data usage.

In case of under the age of 16, to use any service such as online services such as download, and subscription needs their parent or legal guardian approval to use the child’s personal data.

(Your EuropeYour Europe, 2019).

**What are the consequences of not complying with data protection law?**

There is a serious penalty for Companies or organizations that fail to comply with the Data Protection law.

In a situation whereby organizations or companies fail to cooperate and comply with data protection and incur a data breach or loss of personal data will have to face a penalty of up to 4% global annual turn over or 20 million euro.

While that is the Penalty, but it doesn’t end there, there are more Penalties that can be imposed for different types of violation.

Organizations or Companies are given warning provided the infringements are not intentional and the warning is given just once.

The Organization is required to undergo a regular data protection audit.

Audits are taken depending on the scope and application, it usually bases on the review of the official policies while some may be in-depth, and some procedures are implemented.

It is advice able that if an organization does incur data breach, it should notify the relevant authorities with 72 hours to have a chance of avoiding GDPR fines and penalties.

(Eureka, 2019).

**Laws in Relation to storing and processing data and identifying key personnel.**

There are various concepts around monitoring and processing data under the law of GPDR.

* **Personal Data:** The personal data that relates to a living person or that can identify a living person such as names, phone number, bank details and medical history, etc.
* Data subjects: An information subject is the person to whom the individual information relates. You'll be able perused approximately the rights of information subjects in our document
* **Data Controllers:** Information controllers are charac terized within the GDPR as people or associations that, alone or with others, decide the reason and implies of preparing of individual information. Cases of information controllers incorporate restorative experts, banks, government divisions, and intentional associations. A nearby beautician or grocery store may be an information controller if that commerce keeps client subtle elements on file, for case, to create arrangements or to function a special focuses framework.
* **Data processors:** Information processors are people or associations that handle individual information on sake of a controller. Cases of information processors incorporate finance companies and showcase inquire about companies, all of which may hold or handle individual data on sake of an information controller. The GDPR characterizes information preparing as any operation(s) performed on individual information, for case, collecting, putting away, dispersing or crushing.
* **Profiling:** Profiling may be a specific frame of preparing portrayed for the primary time beneath the GDPR. Profiling implies any shape of mechanized preparing of individual information to assess certain individual viewpoints for any individual. For illustration, the preparing of information to examine or anticipate a person's execution at work, financial situation, health, individual inclinations, intrigued, conduct, area or movement. Controllers and processors who carry out profiling got to advise information subjects approximately how the profiling instrument works some time recently handling.

In Relation to the Key personnel, Personal data must be:

* Processed lawfully, transparent and must be fairly used in manners to the data subject
* Data should be specified and must be used for legitimate purpose; it must not be used in manners not compatible with thee data subject.
* Data should only be used for relevant and adequate purpose for which it was collected.
* Data must be secured with an up to date and every reasonable step must be taken to keep data secured and the inaccurate data is securely rectified without delay.
* Data should be protected against unauthorized access, unlawful processing, accidental loss, destruction and damage.

(Citizen Information Centre, 2018 )

**Conclusion**

In conclusion, The Irish data protection and the GDPR plays a big role in taming big companies and organizations from mining and using people’s data without authorizations.

At the same time, they are limiting a lot of things, in other word too many restrictions discourage companies and organization from coming to invest and establish in Europe.

Recently there was an argument about using memes online to be referenced, this is giving the data owner an advantage on earning from their creations, but it is not appropriate for some to have to pay to using emojis and memes online.

# References

Citizen Information Centre. ( 2018 , August 30 ). *Controlling and processing data under the GDPR - concepts and principles* . Retrieved from Citizen Information: https://www.citizensinformation.ie/en/government\_in\_ireland/data\_protection/controlling\_and\_processing\_data\_under\_the\_GDPR.html

Eureka. (2019, 11 26). *GDPR Fines and Penalties – Consequences of Non-Compliance*. Retrieved from Eureka: https://eureka.eu.com/gdpr/penalties-fines/

Your EuropeYour Europe. (2019, 06 14). *Your Europe*. Retrieved from Data protection and online privacy: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index\_en.htm