Meta and Privacy in the European Union

The European Union General Data Protection Regulation (GDPR) was enacted in May 2018. This law governs how personal data of those within the EU may be processed or transferred. The law has a wide scope and is considered one of the toughest security laws in the world. Although passed by the EU, it imposes obligations onto organizations everywhere if they collect or target data related to EU citizens. Each country is responsible for monitoring companies within their jurisdiction through watchdog organizations as well as processing and handling fines. Since its inception, there have been over 900 fines issued across the European Economic Area (EEA) and the U.K. The largest of which is a 746 million euro fine against Amazon handed down by Luxembourg, although an appeal is underway.

The enforcement of the GDPR and a country’s ability to investigate a companies operations has come into question over the last two years. Ireland is responsible for multinational companies such as Google, Facebook, Microsoft, and Twitter and has faced scrutiny due to its economic relationship with the companies and its ability to process and hand down fines. For reference, by the end of 2019, over 160 fines had been enacted while Ireland did not levy a single one. Ireland just handed an $18.6 million fine against Meta Platforms for data breaches that happened in late 2018. Ireland has claimed that proper probes take time because the GDPR is untested, and cases need to meet requirements from all 28 EU Nations, as well as in national court. “It’s going to take as long as it take to do it properly.” A spokesman from the German Watchdog said, “It is absolutely unsatisfactory to see that the biggest alleged data protection violations of the last 15 months with millions of individuals [concerned] are far away from being sanctioned (December 2019).”
The GDPR gives countries the ability to hand down fines on violators as well as allowing injured citizens to seek compensation. The scope of the GDPR gives countries a lot of room to operate and control a company’s practices. In reference to the $18.6 million fines against Meta Platforms, the Data Protection Commission (DPC) of Ireland stated, “that Meta Platforms failed to have in place appropriate technical and organizational measures which would enable it to readily demonstrate the security measures that it implemented in practice to protect EU users’ data.” In a 225 million euro case against WhatsApp, the company “failed to fully communicate to European users how it handled their data, specifically how it shared data with its parent company, Meta Platforms (Facebook). Google was targeted for 50 million euros because they were not transparent on how data was collected and used for advertising. The wide scope of the GDPR has led to variations in how watchdogs are interpreting the rules which leads to discrepancies on who should be charged and what issues are the most pressing.

The GDPR is only a starting point for global data protection, it is supposed to be a model for other countries on how to enact and enforce the data protection of its citizens. It is in its youth, and while the EU works out the kinks that the GDPR has lead to it is learning and improving its data protection, will the world follow?

Questions to Consider?

Is it possible to speed up probes and cut through bureaucratic red tape?

Could the GDPR be applied on a global scale?

Could a uniform standard for what is considered a violation be enacted?

How far can the EU go in fining other country’s companies?

Helpful Links:

https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection#:~:text=The%20EU%20General%20Data%20Protection%20to%20companies%20of%20all%20sizes.