Big Data, Privacy, & GDPR

Key Takeaways

Big data, privacy, and the General Data Protection Regulation (GDPR) are all interconnected in the digital era. Here are some key takeaways to understand their relationship:

Definition and Scale of Big Data: Big data refers to extremely large datasets that are difficult to analyze with traditional methods. These datasets can be harvested from a variety of sources including social media, e-commerce, sensors, and more. Big data analytics offer insights, patterns, and predictions which are invaluable to businesses.

Privacy Concerns: With the increasing amount of data collected, concerns about user privacy have grown. Without proper precautions, big data can be misused to infringe on individual privacy by revealing personal information or patterns.

Enter GDPR: The General Data Protection Regulation (GDPR) was introduced by the European Union (EU) in 2018 to address privacy concerns. It sets guidelines for the collection and processing of personal information of individuals within the EU.

Consent is Key: Under GDPR, organizations must obtain explicit and informed consent from individuals before collecting and processing their data. This means clear communication without relying on pre-ticked boxes or buried clauses in terms and conditions.

Right to Be Forgotten: GDPR introduced the "right to be forgotten," meaning individuals can request organizations to delete their personal data.

Data Portability: Another key provision in the GDPR is the right to data portability, allowing individuals to request a copy of their personal data in a format that allows for easy movement between different service providers.

Penalties: Non-compliance with GDPR can result in hefty fines, up to €20 million or 4% of the annual worldwide turnover of the preceding financial year, whichever is higher.

Impact Beyond EU: Even though GDPR is an EU regulation, it has a global impact. Any company, regardless of location, that deals with the data of EU citizens must comply.

Anonymization and Pseudonymization: To work with big data while ensuring privacy, techniques like data anonymization (where data is rendered anonymous) and pseudonymization (where data can't be attributed to a specific data subject without additional information) are essential.

Data Protection Officers (DPOs): GDPR recommends or mandates (depending on the scale and type of data processing) the appointment of a DPO to oversee the data protection strategy and its implementation.

Data Breaches: Organizations are required to report certain types of data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach.

Emphasis on Accountability: The GDPR mandates that organizations not only comply with its provisions but also demonstrate their compliance. This means having clear policies, procedures, and records of data processing activities.

Tech and AI Concerns: As AI and machine learning become more integrated with big data, there are increasing concerns about automated decisions, profiling, and the potential bias in algorithms. GDPR provides rights for individuals to not be subject to decisions based solely on automated processing in certain cases.

As big data continues to grow in importance, understanding and complying with regulations like GDPR becomes crucial for businesses. It represents a shift towards prioritizing user privacy and giving individuals more control over their data in the digital age.

Case Study: A GDPR Fine in Romania

The following material is available on the website of the National Supervisory Authority for Personal Data Processing at:

https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_09.08.2022_2&lang=en

The National Supervisory Authority finalized in July 2022 an investigation at the controller DN SRL and found the breach of the provisions of Article 12, Article 13, as well as those of Article 5 paragraph (1) letters a), b) and c), by reference to Article 5 paragraph (2) and Article 6 of the General Data Protection Regulation.

Therefore, the controller was sanctioned as it follows:

- **fine in amount of lei 4,945.1 (the equivalent of EUR 1,000)** for the breach of the provisions of Articles 12-13 of the General Data protection Regulation;
- **fine in amount of Lei 7,417.65 (the equivalent of EUR 1,500)** for the breach of the provisions of Article 5 paragraph (1) letters a), b) and c), by reference to Article 5 paragraph (2) and Article 6 of the General Data protection Regulation.

At the same time, based on Article 58 paragraph (2) letter d) of the General Data Protection Regulation, the following **corrective measures** were taken against the controller:

1. providing the information of the data subjects through the communication in a concise, transparent, intelligible and easily accessible form of all information provided under Article 13 of the General Data Protection Regulation and subject to the transparency conditions mentioned under Article 12 of the same Regulation;

2. the elimination of the use of the video surveillance camera existing within the cosmetic room for which there is no specific legal ground for the processing of the clients' personal data and of its employees according to Article 6 of the General Data Protection Regulation;

3. ensuring the compliance of the personal data processing operations with the General Data Protection Regulation, through the implementation of some adequate technical ad organisational measures and the establishment of some adequate rules relating to the management of the images registered by the surveillance cameras;

4. the interdiction of the remote access through internet to the images and registrations, as well as the access of the images and registrations solely in case of accident in relation to the purpose of the video surveillance cameras instalment.

The investigation was started following an intimation through which a natural person noticed that there were data subjects, clients of **DN SRL**, which were under video surveillance during the performance of some cosmetic services.

Within the investigation performed, it was found that the controller **DN SRL** holds a video surveillance system installed both inside, as well as outside the space where the controller carries out its activity, that monitors both the employees and clients.

Also, it was found that the controller did not prove that it performed **a clear, complete and accurate information of its employees and of the data subjects whose personal data (respectively the image) are processed through the video surveillance cameras**, by communicating all the information provided under Article 13 of the General Data Protection Regulation and subject to the transparency conditions from Article 12 of the same regulation.

At the same time, it resulted that **DN SRL** did not provided any proofs of some previous existing incidents in order to justify its legitimate interest that prevails over the interests or fundamental rights and freedoms of the data subjects. Therefore, it was found that the controller excessively processed the data (images) of its clients and employees, through the video camera installed in the location where the cosmetic treatments were performed. The data thus processed were not adequate, relevant and limited to what is necessary by reference to the purposes for which they were processed (“data minimisation”). The purpose declared by the controller could have been achieved through less intrusive means for the privacy of its clients and employees.

Therefore, the breach of the provisions of Article 5 paragraph (1) letters a), b) and c) of the General Data Protection Regulation by reference to the conditions regarding the lawfulness of the processing established under Article 6 of the same regulation was found.

Moreover, the controller was not able to prove the observance of the processing principles according to Article 5 paragraph (2) of the General Data Protection Regulation.

Further Reading

European Union. (2023). *What is GDPR, the EU's new data protection law?*

https://gdpr.eu/what-is-gdpr/

Payton, T., & Claypoole, T. (2023). *Privacy in the age of Big data: Recognizing threats, defending your rights, and protecting your family*. Rowman & Littlefield.

https://rowman.com/ISBN/9781442242579/Privacy-in-the-Age-of-Big-Data-Recognizing-Threats-Defending-Your-Rights-and-Protecting-Your-Family

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, *25*(1), 37-43.

https://www.nature.com/articles/s41591-018-0272-7

Robertson, V. H. (2020). Excessive data collection: privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1).

https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/57.1/COLA2020006