ЭРДЭМТЭН, СУДЛААЧДЫН ҮЗЭЛ БОДОЛ

FRAMEWORK OF THE EUROPEAN DATA PROTECTION LAW

Namsrai Battulga
Ph.D. student at University of Pecs, Hungary

Abstract: Personal data protection policy is defined as granting individuals a right to control the nature, content, and circulation of information. However, data storage and protection structures vary from country to country. For the European Union, this policy is moving forward more steadily.

Keywords: *public record, personal consent, unduplicated data.*

Data is an intangible asset, and social interaction consists of data fusion and information-based decision-making. Thus technological advances are accelerating community, institutional, and personal data proactive in the long run.

If personal information was mainly owned by the state, but today, the freedom[117] of using, and sharing personal data with others is enhanced as well. With the reference to countries, they are not limiting the aforementioned freedom as much as possible but follow the policy of improving the legal framework.

The process has advanced over the last 40 years, with the United Nations and the Organization for Economic co-operation and development issuing guidelines on personal data privacy, storage, and data flow since 1981. According to the data privacy, ethics, and protection guidance note on big data for achievement of the 2030 agenda:

Data access, analysis, or other use must be consistent with the United Nations Charter and in furtherance of the sustainable development Goals. Whether directly or through a contract with a third-party data provider, data should be obtained, collected, analyzed, or otherwise used through lawful, legitimate, and fair means.

"In particular, data access (or collection, where applicable), analysis or other use should be in compliance with applicable acts, including data privacy and data protection laws, as well as the highest standards of confidentiality and moral and ethical conduct. Legally binding agreements outlining parameters for data access and handling (e.g. data security, data formats, data transmission, fusion, analysis, validation, storage, retention, re-use, licensing, etc.) should be established to ensure reliable and secure access to data provided by third-party collaborators." (*Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda*, sec.3)

As regards the European Union first adopted the data protection directive in 1989, and also updated it in 2016, gradually releasing rules aimed at ensuring the confidentiality of data related to credit information, public records, and e-commerce databases, and prohibiting illegal use. "The goals of the EU Directive on Data protection are to facilitate the free flow of data throughout the European Union while ensuring a high level of protection of the rights of data subjects. Besides giving individuals the right to prevent the use of their personal data for direct marketing purposes, the directive also provides the right to access and correct personal information. The directive imposes very strict rules regarding sensitive information such as ethnic and racial origin, political and religious beliefs, union membership, sexual orientation, and health." (*Mark J. Smith and others, European law*, p.698)

[117] Personal rights are guaranteed by national constitutions and the European Convention on Human Rights, and, on the other hand, the fundamental freedoms are enshrined in the EC Treaty. In addition, the conflict between private law and fundamental rights arises because of the perceived tension between party autonomy, on the one hand, that is, the right of any private person to choose which transaction to conclude, with whom, and on what terms–and, on the other hand, the limitations on this that the various fundamental rights could impose. "See details", Kristian Twigg-Flesner, A key features of European Union Private law, p.10

The legal framework for data protection consists of directives as well as other regulations. It includes:

- Directive 95/46/EC defined principles on data-processing such as whether they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy.

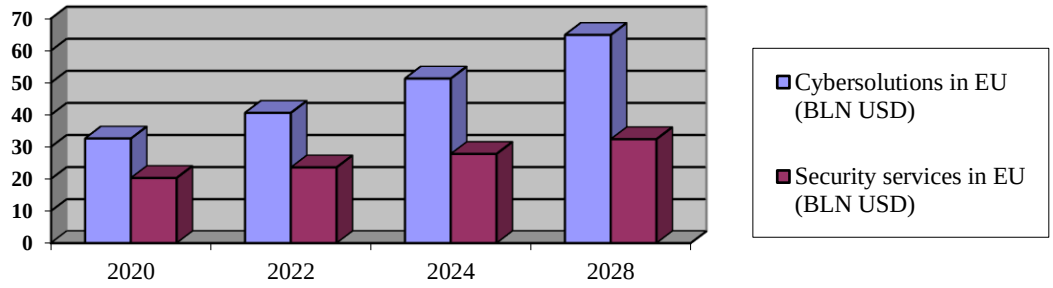
- Directive 2000/31/EC of the European Parliament aims at improving the functioning of the internal market with respect to online commerce. Directives contain the regulation concerning the data requirements of service providers as well.

- European Commission Regulation 330/2010 defines records data processing, submitting data breach notifications or data protection impact assessments, and has notably extended obligations regarding the handling of data subjects' requests.

- General Data Protection Regulation (2016/679) and the Law Enforcement Directive (2016/680) with a set of harmonized rules applicable to the design, development, and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems.

Furthermore, European Commission declares a country "data protection safe" because of GDPR. It protects the personal privacy rights of EU residents and businesses. In other words, it makes organizations accountable for personal data protection. This includes having security measures in place to guard against data breaches and taking quick action to notify individuals and authorities in the event a breach does occur. This platform gives the opportunity to holistically reassess all the data.[118]

In Europe, driven by the increasing awareness of data risks and threats, the global Cyber security market has witnessed robust growth over the last years with revenue increased. Revenue is expected to show an annual growth rate of 12.54 percent, resulting in a market volume of 73.3 billion USD by 2027. (*https://www.statista.com/outlook/tmo/cybersecurity/europe#revenue*)



With the improvement of the legal framework of data protection, business and information, communication, and electronic operators in the economic bloc of the European Union have a wide opportunity to collect and analyze any data and diversify customer services.

Under the Common European Sales law, digital content is often supplied not in exchange for a price but in combination with separate paid goods or services, involving a non-monetary consideration such as giving access to personal data or free of charge in the context of a marketing strategy based on the expectation that the consumer will purchase additional or more sophisticated digital content products at a later stage.[119]

[118] "See details", Aleksandra Danielewickz, Ensuring GDPR compliance can boost your business, 2021

[119] The buyer may only claim damages for loss or damage caused to the buyer's property, including hardware, software, and data, by the lack of conformity of the supplied digital content, except for any gain of which the buyer has been deprived by that damage. "See details", Regulation of the European Parliament and of the Council on a Common European Sales law, 2011/0282, Art.107

Namely, a business entity creates a customer database to organize its services quickly. This database includes the user's name, age, gender, home address, contact email, phone number, and account number. Some institutions, such as banks and insurance, law enforcement[120], security companies, create a fund by taking unduplicated customer information such as fingerprints.

The right to store this information is granted by the user to the business owner, and on the other hand, the contracting party undertakes not to disclose the information and to use it only for the user. In terms of general legal regulations, parties to the contract are prohibited from transmitting information on behalf of others in any form.

The legal framework of the European Union has a wide range of regulations, including fair access to data, use for mutually agreed purposes, and deletion once the purpose has been met. The data protection framework consists of information encryption, data transfer and cross-border data flow control, and data protection impact assessment.

"According to EU constitution policy, article 49 requires transparency of the proceedings of Union Institutions whereas article 50 protects personal data." (*Jürgen Schwarze, Enlargement, the European Constitution, and Administrative Law*, p.980)

The EU member states are responsible for appointing independent organizations and officials[121] to monitor the activities of knowing, accessing, correcting, and deleting information, and guaranteeing the rights of the data owner in accordance with domestic laws.[122]

As regard, the requirements are to process the data only on the grounds and to the extent stipulated by the law, or according to the consent given by the data owner, to stop the data collection immediately if it is refused, to check the accuracy and completeness of the data, and to monitor the requirements.

While member states adhere to the principles of data protection, the traditional regulations on limiting the use, collection, and exchange of data for the purpose of ensuring national security, as well as keeping government activities open to the public and officials' incomes, remain in the former platform.[123] Also, without violating the rights and legal interests of others, taking into account their demands and needs, in order to support the economy and business, develop research and analysis work, and increase the transparency and availability of information, the form of general overview can be made open data.

Conclusion

Part of this century's fastest-growing virtual social interaction is the process of collecting, handling, using, and securing data with the help of hardware and software. Biometric information such as fingerprints, face, voice recognition, genetics, communication, wealth, income, religion, beliefs, sexual orientation, and other personal information of a person, except for ensuring national and public security[124] should be unassailable.

---

[120] All remote biometric identification systems are considered high risk and subject to strict requirements. Such use is subject to authorization by a judicial or other independent body and to appropriate limits in time, geographic reach and the databases searched. "See details", EU Commission Proposal for Artificial intelligence act and amending certain union legislative acts. 2.1. 2021/0106

[121] Data access should be limited to authorized personnel, based on the "need-to-know" principle. Personnel should undergo regular and systematic data privacy and data security trainings. Prior to data use, vulnerabilities of the security system (including data storage, way of transfer, etc.) should be assessed. "See details", Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda, UN

[122] An example, the Italian Parliament passed legislation on data protection, with a new law implementing the EU Directive on Data Protection. In some respects, this law is stricter than the EU Directive. In Particular, the owner of the data has various duties regarding notification, obtaining consent, and ensuring data confidentiality. Criminal and civil sanctions apply to breaches of this law. "See details", Mark J. Smith and others, European law, p.703

[123] As of today, 110 countries in the world have data protection laws. In addition, about 30 countries are making efforts to adopt this type of law. "See details", *National comprehensive data protection/privacy laws and bills*.

[124] Also, the confidentiality of trade data will have to be assessed in light of newer legal avenues for access to such data for law enforcement, and anti-terrorism initiatives. "See details", Hal Burman, Private International Law, p.754

The legal framework is not just about data protection. Moreover, the choice of data sharing is an individual right. If the information is collected with personal consent, it shall be used to provide information that is useful to a person in accordance with a contract.

This principle is a vital interest of the regulation, not only in the European Union but also worldwide. In any form, the data receiver must obtain permission from the data owner to process, collect, and use the data, as well as report on the legality and security of these transactions and activities, including government oversight. The form of control should not only be legislation but flexible management and organizational policies and regulations should be implemented.

Within the framework of this policy, European Union directions and regulations are aimed at preventing illegal data collection, monitoring and evaluating integrity, and confidentiality. And the availability of information systems used for data collection, processing, and use, developing measures to be taken in the event of data loss, and limiting the use of data, and procedures. Those instructions are being adopted to delete information and make it impossible to identify the owner of the information.

Along with this extensive process, there will undoubtedly be steps to increase and diversify legal responsibilities on how to promptly investigate and resolve any complaints related to data collection, processing, and use at the European Union and member state level. In short, they are closely looking at the current situation while developing future policies.

REFERENCES

Aleksandra Danielewickz, Ensuring GDPR compliance can boost your business, 2021

Data privacy, ethics and protection guidance note on big data for achievement of the 2030 agenda, UN, 2017

Directive 2000/31/EC

Directive 95/46/EC

EU Commission Proposal for Artificial intelligence act and amending certain union legislative acts. 2021/0106

European Commission Regulation 330/2010

General Data Protection Regulation 2016/679

Hal Burman, Private International Law, 2009

Jürgen Schwarze, *Enlargement, the European Constitution, and Administrative Law,* 2004, The International and Comparative Law, Vol. 53

Kristian Twigg-Flesner, A key features of European Union Private Law, 2014

Mark J. Smith and others, European law, 1999

National comprehensive data protection/privacy laws and bills, 2019

Regulation of the European Parliament and of the Council on a Common European Sales law, 2011/0282

The Law Enforcement Directive 2016/680