Let's Talk About Data Protection

We have been living in the information era for some time now, and today, data is the most valuable resource. It is vital to understand that every action, decision, and movement we make generates data, and this has become inevitable. It is through data that businesses are built, decisions are made, and relationships are established. Given its significance, it is imperative to discuss data protection, which has become a recurring concern among governments, organizations, and individuals alike. We aim to provide a perspective from both the Dominican Republic and the international scene, focusing on regulatory aspects and the most recent significant cases.

1. Data Privacy Legislation:

1. Dominican Republic: The main rule is Law No. 172-13 for the Protection of Personal Data.

2. Europe: The key regulatory framework is the General Data Protection Regulation (GDPR), applicable across all European Union member states.

3. United States: Unlike Europe, the US does not have a single federal data protection law. However, laws like the California Consumer Privacy Act (CCPA) in California and the Health Insurance Portability and Accountability Act (HIPAA) for the health sector regulate specific aspects of data protection.

2. Guiding Principles:

1. Dominican Republic and Europe: Both legislations share principles such as lawfulness, loyalty, purpose limitation, accuracy, and data retention limitation.

2. United States: While there is no unified regulation, principles like transparency, purpose, and data minimization frequently emerge in various state and federal laws.

3. Rights of the Data Subject:

1. Dominican Republic: ARCO rights (Access, Rectification, Cancellation, and Opposition) are recognized.

2. Europe (GDPR): Citizens' rights are expanded, including the right to be forgotten, data portability, and the right to be informed about data breaches.

3. United States: Depends on the jurisdiction and specific law, but for instance, the CCPA grants rights similar to the GDPR, such as access, opposition to data sale, and deletion.

4. Organization's Responsibilities:

1. Dominican Republic: Entities must inform, maintain confidentiality, secure data, and register files with the controlling authority.

Av. John F. Kennedy 64, Santo Domingo, D.N. 10512, República Dominicana • 809.566.7111 • www.ulisescabrera.com • info@ulisescabrera.com • RNC 1-01-88634-1

2. Europe (GDPR): Organizations must ensure GDPR principle compliance, conduct Data Protection Impact Assessments in certain cases, and appoint a Data Protection Officer when necessary.

3. United States: Responsibilities vary, but many laws require transparency, informed consent, and adequate security measures.

5. International Data Transfer:

1. Dominican Republic: International data transfer is permitted under certain conditions, safeguarding adequate data protection.

2. Europe (GDPR): Transfers outside the EU are subject to stringent requirements to ensure an adequate level of protection.

3. United States: Transfers are more based on bilateral or sectoral agreements. A key example was the "Privacy Shield" between the EU and the US, although it was invalidated by the Court of Justice of the EU in 2020.

6. Regulatory Approach and Sanctions:

1. Dominican Republic: The law establishes sanctions including fines and the possibility of suspension of activities related to data processing.

2. Europe (GDPR): Highly regulatory approach, with sanctions reaching up to 4% of the company's global annual turnover or 20 million euros, whichever is greater.

3. United States: The approach varies by state and sector, generally combining civil penalties, notification requirements, and in some cases, class actions by consumers.

7. EU GDPR Casebook

Since the implementation of the GDPR in the EU in May 2018, there have been several notable penalties imposed on companies for violations:

France: Google. In 2019, the National Commission on Informatics and Liberty of France (CNIL) imposed a fine of 50 million euros on Google. According to the CNIL, Google did not provide clear and understandable information to its users about how it processes their data and did not obtain valid consent for the personalization of its advertisements.

United Kingdom: British Airways. In an active 2019, the Information Commissioner's Office (ICO) of the United Kingdom initially announced its intention to fine British Airways 204 million euros due to a data breach that affected approximately 500,000 customers. However, the fine was later reduced to 22 million euros in 2020, partly due to the economic repercussions of the COVID-19 pandemic and the representations made by British Airways.

United Kingdom: Marriott International. The ICO also announced in 2019 a proposed fine of 110 million euros for Marriott International due to a data breach that exposed the personal information of up to 339 million guests. As with British Airways, the fine was later reduced to 20 million euros in 2020.

Italy: TIM. In 2020, the Italian Data Protection Authority imposed a fine of 27.8 million euros on TIM, one of Italy's leading telecommunications companies, for various infractions, including unsolicited marketing and data processing failures.

Germany: H&M. In 2020, the data protection authority of Hamburg imposed a fine of 35.3 million euros on the German subsidiary of the fashion brand H&M. The company had stored private information about its employees in a file accessible to hundreds of managers.

Ireland: WhatsApp. In 2021, WhatsApp was fined 225 million euros by the Data Protection Commission of Ireland due to a lack of transparency about how it shares data with other Facebook companies.

In closer latitudes:

Colombia: Uber. In 2019, the Superintendency of Industry and Commerce (SIC) fined Uber approximately 2.128 billion Colombian pesos (about 600,000 dollars) due to a data breach that affected 267,000 Colombians in 2016.

Mexico: Banco Mercantil del Norte (Banorte). In 2013, the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) imposed a fine of 32 million Mexican pesos (about 1.6 million dollars) on Banorte for not adequately protecting its customers' data.

Argentina: Telefónica Móviles Argentina. In 2017, the National Directorate of Personal Data Protection imposed a fine of 110,000 Argentine pesos (about 1,200 dollars) for not correctly updating the database of the 'Do Not Call' system, allowing users to continue receiving unwanted advertising.

Chile: Retail Financiero (CMR Falabella). In 2019, the Superintendency of Banks and Financial Institutions imposed a fine of 6,000 UF (about 170,000 dollars) on CMR Falabella for not timely reporting a data leak that affected more than 14,000 credit cards.

Peru: Supermercados Peruanos (Plaza Vea). In 2018, the National Authority for the Protection of Personal Data fined the company 183,000 soles (about 55,000 dollars) for not having the explicit consent of its customers for the processing of their personal data in marketing actions.

These are just some examples of sanctions related to the EU GDPR and other jurisdictions. It is important to highlight that each case has unique and specific circumstances, the extent of the violation, and other factors determine the severity of the sanctions. Furthermore, many of these sanctions may be subject to appeal or negotiation. In Latin America, the willingness of authorities to guarantee the privacy and security of the personal information of citizens is clear. It is essential that companies in the region are aware of their obligations and act proactively to avoid sanctions and ensure the trust of their customers and users.

Av. John F. Kennedy 64, Santo Domingo, D.N. 10512, República Dominicana • 809.566.7111 • www.ulisescabrera.com • info@ulisescabrera.com • RNC 1-01-88634-1

In our own backyard, the Dominican Republic has worked on strengthening its legal framework related to the protection of personal data, especially through Law No. 172-13 for the Protection of Personal Data. However, despite discussions and awareness-raising activities around this law, the application of specific sanctions has not been as prominent as in other jurisdictions.

8. Final Remarks

Although there are differences in the way the Dominican Republic, Europe, and the United States approach data privacy and protection, all recognize the fundamental importance of protecting the rights of individuals in relation to their personal information. In an increasingly interconnected world, harmonization and understanding of these regulations become essential for organizations operating globally.

In our digital era, information, or 'data', has become the most valuable resource. We are generators of data, consumers of it, we commercialize it, and often, we are vulnerable to its misuse. Its increasing relevance compels us to understand and discuss the data protection landscape, both in the Dominican context and internationally.

This brief article has aimed to provide more than just an opinion; it aims to present a regulatory perspective, highlighting significant cases and critical aspects in the realm of data protection. With the hope of having offered clarity and understanding on this complex and constantly evolving topic, we invite readers to reflect on the importance of these regulations in our current digital society.

Author:
MÓNICA VILLAFAÑA
Partner

*This summary contains only general information on the topics covered, so this document does not constitute a legal opinion. Ulises Cabrera recommends seeking specific legal advice for each case.