COMMUNITY REGULATIONS REGARDING THE PROTECTION OF PERSONAL DATA

Olivia DULSCHI,
master în științe politice,
arhitect de date și business intellegence,
Londra, Marea Britanie

In an era defined by advanced technology and interconnectedness, the handling and protection of personal data have emerged as critical issues of paramount importance. Individuals, organisations, and governments worldwide are grappling with the challenge of striking a delicate balance between leveraging the benefits of data-driven advancements and safeguarding the fundamental rights and privacy of individuals. As personal data becomes an increasingly asset, it is imperative to establish robust policies and regulations at both the national and international levels to ensure the responsible and ethical use of such information. This report delves into the intricate landscape of national and international policies and regulations governing the protection of personal data. It aims to provide a comprehensive overview of the evolving legal frameworks, best practices, and key considerations that shape the landscape of personal data protection worldwide. By examining the approaches taken by different countries and international bodies, we can gain insights into the diverse strategies and challenges involved in safeguarding personal data in today's digital age. The reports begins by exploring the fundamental concepts and principles underpinning personal data protection, including the notions of privacy, consent, and data minimisation.

We will then delve into an examination of national policies and regulations, displaying the diverse approaches adopted by countries around the world. By analysing specific case studies and legislative frameworks, we can gain a deeper understanding of the strategies employed to protect personal data within different authorities. Furthermore, this report will investigate the ever-growing influence of international regulations on personal data protection. Notably, the General Data Protection Regulation (GDPR) enacted by the European Union (EU) has set a global benchmark for data protection standards and influenced the legal landscape beyond its authority. We will explore the impact of the GDPR and other international frameworks, highlighting the challenges and opportunities they present for both individuals and organisations operating in a globalised data ecosystem. Lastly, the report will address emerging trends and future directions in the field of personal data protection. As technological advancements continue to reshape the digital landscape, novel challenges such as artificial intelligence, big data analytics, and the Internet of Things (IoT) pose new risks to personal data security. By examining ongoing discussions and initiatives at the national and international levels, we can gain insights into the strategies being developed to adapt and enhance personal data protection in the face of these evolving technologies.

The European Union has played a pivotal role in shaping data protection regulations through the introduction of various directives. These directives establish a harmonised

framework across EU member states, ensuring consistent standards for the protection of personal data. Here are some key EU directives in the field of data protection:

1. Data Protection Directive 95/46/EC: Enacted in 1995, this directive was a significant milestone in data protection within the European Union. It established fundamental principles and regulations governing the processing of personal data. The directive introduced key concepts, such as data subject rights, the responsibilities of data controllers and processors, and guidelines for cross-border data transfers. It formed the basis for national data protection laws in EU member states until the implementation of the GDPR[1].

2. ePrivacy Directive 2002/58/EC: Commonly known as the Cookie Directive, this directive addresses privacy concerns in electronic communications. It focuses on safeguarding individuals› privacy in various electronic communication services, including email, SMS, and online platforms. The directive specifically addresses the use of cookies and similar tracking technologies, requiring explicit consent from users before storing or accessing information on their devices[2]**.**

3. Data Retention Directive 2006/24/EC: The Data Retention Directive aimed to standardise data retention obligations across EU member states. It mandated telecommunication providers to retain certain metadata, such as the source, destination, date, time, and duration of communication, for a specified period. The objective was to assist law enforcement agencies in investigations and the prevention of serious crimes. However, the directive was later invalidated by the Court of Justice of the European Union (CJEU) in 2014 due to concerns regarding its indiscriminate and disproportionate nature[3].

4. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679): The GDPR, enforced from May 25, 2018, represents a significant advancement in data protection legislation. It replaced the Data Protection Directive 95/46/EC and introduced a comprehensive and harmonized approach to data protection across the EU. The GDPR strengthens individual rights, imposes stricter obligations on data controllers and processors, and introduces stringent rules for personal data processing. Notable provisions include the right to erasure (right to be forgotten), the right to data portability, and the requirement for data protection impact assessments. Non-compliance with the GDPR can result in severe penalties, with fines of up to 4% of global annual turnover or €20 million, whichever is higher[4].

5. ePrivacy Regulation (under development): The ePrivacy Regulation is current-

[1] eur-lex.europa.eu. (n.d.). Directive 95/46/EC of the European Parliament and of the Cou... - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:31995L0046.

[2] eur-lex.europa.eu. (n.d.). EUR-Lex - 32002L0058 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.

[3] Legislation.gov.uk. (2020). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. [online] Available at: https://www.legislation.gov.uk/eudr/2006/24/contents.

[4]Legislation.gov.uk. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). [online] Available at: https://www.legislation.gov.uk/eur/2016/679/contents.

ly being developed to replace the outdated ePrivacy Directive 2002/58/EC[5]. It aims to align privacy and confidentiality rules in electronic communications with the GDPR. The regulation will address various aspects, including direct marketing regulations, consent requirements for tracking technologies, and the protection of communication privacy. Its goal is to empower individuals with greater control over their electronic communications and establish a robust data protection framework in the digital realm. These EU directives, along with the GDPR and the forthcoming ePrivacy Regulation, demonstrate the EU›s commitment to protecting personal data and privacy rights. They contribute to a comprehensive and harmonized legal framework that promotes responsible and transparent data processing practices throughout the European Union. In the upcoming paragraphs, we will delve into a comprehensive analysis of the legal framework surrounding the General Data Protection Regulation (GDPR) and its far-reaching implications.

GDPR – The Regulation that Shifted the Global View of Digital Privacy.

The implementation of the General Data Protection Regulation (GDPR) on May 25, 2018, brought about a significant transformation in the European Union›s (EU) data protection and privacy regulations. This regulation introduced a unified and rigorous framework for the handling of personal data across all EU member states. By examining the fundamental elements and provisions of the GDPR, we can develop a deeper comprehension of its legal foundations and the substantial impact it has had on businesses, organisations, and individuals alike.

The GDPR is an extensive and wide-ranging legal framework that governs the collection, processing, storage, and transfer of personal data of individuals within the European Union (EU) and the European Economic Area (EEA) by organisations. Its primary objective is to enhance the privacy, security, and control that individuals have over their personal data. Additionally, the GDPR aims to harmonise and simplify the regulatory environment for international businesses involved in data processing within the EU or the EEA. The GDPR applies to any organisation, regardless of its geographical location, that:

- Offers goods or services to individuals in the EU or the EEA, or
- Monitors the behaviour of individuals in the EU or the EEA.

Consequently, the GDPR›s reach extends globally and impacts numerous organisations outside of Europe that oversee personal data of European individuals. According to the GDPR, personal data is defined as any information related to an identified or identifiable natural person. This encompasses not only explicit identifiers like name, address, email, and phone number, but also less obvious ones such as IP address, cookie identifier, location data, biometric data, genetic data, and more. Furthermore, the GDPR acknowledges special categories of personal data that are more sensitive and require heightened protection, such as data concerning race, ethnicity, political opinions, religious beliefs, health, sex life, sexual orientation, and more[1]. The GDPR establishes a set of principles and rules that organisations must adhere to when processing personal data.

[5] digital-strategy.ec.europa.eu. (n.d.). ePrivacy Regulation | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

These principles include:

- Lawfulness, fairness, and transparency: organisations must have a valid legal basis, such as consent, contract, legal obligation, vital interest, public interest, or legitimate interest, to process personal data. Additionally, organisations must inform individuals about the purposes, extent, and duration of the processing, as well as their rights and choices regarding their data.

- Purpose limitation: organisations must only process personal data for specific, explicit, and legitimate purposes that are compatible with the original purpose for which the data was collected.

- Data minimisation: organisations must only process personal data that is adequate, relevant, and limited to what is necessary for the intended purposes.

- Accuracy: organisations must ensure the accuracy of personal data and, if necessary, update or rectify inaccurate or incomplete data without delay.

- Storage limitation: organisations must retain personal data only for as long as necessary for the intended purposes of processing. They must also establish and implement retention policies and procedures for deleting or anonymizing personal data when it is no longer needed.

- Integrity and confidentiality: organisations must process personal data in a manner that ensures appropriate security, protecting against unauthorised or unlawful processing, accidental loss, destruction, or damage. They must adopt technical and organizational measures, such as encryption, pseudonymization, and access control, to safeguard personal data.

- Accountability: organisations must demonstrate compliance with the GDPR and its principles.

They must integrate data protection by design and by default, meaning they must consider and incorporate data protection into every aspect of their data processing activities from start to finish. The GDPR also grants individuals various rights concerning their personal data. These encompass:

- Right to access: Individuals possess the entitlement to confirm whether organisations are processing their personal data and, if so, access that data and receive information about the processing.

- Right to rectification: Individuals have the right to request the correction of any inaccurate or incomplete personal data concerning them from organisations without undue delay.

- Right to erasure (right to be forgotten): Individuals can request the deletion of their personal data from organisations under specific circumstances, such as when the data is no longer necessary, when consent is withdrawn, or when the processing is unlawful.

- Right to restriction of processing: Individuals can ask organisations to limit the processing of their personal data in certain situations, such as when the accuracy, lawfulness, or necessity of the processing is disputed.

- Right to data portability: Individuals have the right to receive their personal data from organisations in a format that is structured, commonly used, and machine-readable, and to transmit or request the transfer of their data to another organization, where technically feasible.

- Right to object: Individuals can object to the processing of their personal data for specific purposes, such as direct marketing or profiling, based on legitimate interest or consent.

- Right not to be subject to automated decision-making, including profiling: Individuals have the right to avoid being subjected to decisions that are based solely on automated processing and that have legal or significant effects on them, unless specific conditions are met.

Furthermore, the GDPR imposes obligations and responsibilities on different entities involved in data processing, including:

- Controllers: These entities determine the purposes and means of processing personal data and are responsible for compliance with the GDPR, protecting individuals› rights, implementing security measures, conducting assessments, appointing data protection officers (where required), cooperating with supervisory authorities, and reporting data breaches.

- Processors: These entities process personal data on behalf of controllers and must follow their instructions, establish contracts specifying their obligations, implement security measures, assist controllers in fulfilling GDPR requirements, appoint data protection officers (where required), cooperate with supervisory authorities, and report data breaches.

- Joint controllers: When two or more controllers jointly determine the purposes and means of processing, they must establish an arrangement specifying their respective roles, responsibilities, and means of ensuring individuals› rights.

- Representatives: Controllers or processors not established in the EU must appoint representatives in the EU to function as points of contact for individuals and supervisory authorities, and to assist with GDPR-related matters.

- Data protection officers (DPOs): Controllers and processors may need to appoint DPOs with expertise in data protection, who advise and monitor compliance, provide guidance, cooperate with su pervisory authorities, and function as contact points for individuals and authorities.

- Supervisory authorities: These independent public authorities in each EU member state oversee and enforce GDPR compliance, including issuing guidance, conducting investigations, imposing fines, handling complaints, and cooperating with other supervisory authorities.

- European Data Protection Board (EDPB): The EDPB ensures consistent application of the GDPR throughout the EU and EEA, with responsibilities such as issuing guidelines, making binding decisions in disputes between supervisory authorities, approving codes of conduct and certification mechanisms, and advising the European Commission. The GDPR also establishes a system of penalties and remedies for cases of non-compliance and violations of the regulation.

These measures include:

- Administrative fines: Supervisory authorities have the authority to impose fines on controllers and processors who breach the GDPR. The fines can reach up to twenty million euros or 4% of the global annual turnover (whichever is higher) for severe violations such as disregarding processing principles, infringing individuals› rights,

or violating rules on data transfers to third countries. For less severe infringements like record-keeping failures, lack of cooperation with supervisory authorities, or insufficient security measures, fines can be up to ten million euros or 2% of the global annual turnover. The amount of the fine considers factors such as the nature, gravity, and duration of the infringement, intentionality, mitigation efforts, cooperation with authorities, etc.

- *Corrective measures:* Supervisory authorities have the power to impose corrective actions on controllers and processors who violate the GDPR. These measures may include issuing warnings or reprimands, requiring compliance with individuals› requests, imposing restrictions or bans on data processing, suspending data transfers to third countries, revoking certifications or codes of conduct, and more.

- *Compensation:* Individuals have the right to receive compensation from controllers or processors for any material or non-material damages they suffer due to GDPR violations. Controllers and processors are held liable for damages caused by non-compliant processing. Controllers are also responsible for damages caused by processors acting on their behalf, unless they can prove they are not at fault.

- *Judicial remedies:* Individuals can file complaints with supervisory authorities if they believe their personal data processing infringes the GDPR. They also have the right to seek judicial remedies against binding decisions made by supervisory authorities or against controllers/processors if their GDPR rights have been violated[6]. The GDPR is a comprehensive and intricate regulation that significantly impacts data protection and privacy practices in Europe and beyond. It imposes strict standards and obligations on organisations overseeing personal data of individuals in the EU or EEA while granting individuals extensive rights and control over their data. Non-compliance with the GDPR can result in severe penalties and reputational damage for organisations.

Therefore, it is crucial for organisations to understand and adhere to the GDPR, taking an initiative-taking and responsible approach to data protection and privacy[7]. The GDPR is a ground-breaking regulation designed to safeguard personal data and privacy of individuals in the EU and EEA. It establishes a comprehensive framework of principles, rules, rights, and obligations for processing personal data. Additionally, it implements a system of sanctions and remedies to ensure compliance and enforcement. With its global reach, the GDPR affects organisations worldwide that oversee personal data of EU individuals. It signifies a significant shift in the data protection and privacy landscape, requiring organisations to embrace proactive and responsible practices. The GDPR empowers individuals to exercise control over their data and seek remedies for violations. While the GDPR presents challenges and opportunities, it is crucial for organisations to understand, comply with, and respect the rights and interests of individuals regarding their personal data[8].

---

[6] Custers, B., Van der Hof, S., Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy & Internet, Vol. 6, No. 3, pp. 268–295; Custers, B.H.M., and Bachlechner, D. (2018) Advancing the EU Data Economy; Conditions for Realizing the Full Potential of Data Reuse, Information Polity, https://doi.org/10.3233/ip170419.

[7] GDPR (2018). General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

[8] GDPR (2018). General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

Challenges and Downsides of the GDPR: A Comprehensive Analysis

As covered above GDPR has undoubtedly brought significant improvements in data protection and privacy. However, it is not without its challenges and downsides. This report aims to provide an analysis of the key challenges and potential drawbacks associated with the implementation of the GDPR.

Complexity and Compliance Burden. One of the primary challenges of the GDPR is its complexity. The regulation consists of numerous provisions, principles, and requirements that organisations must understand and implement correctly. Achieving compliance with such a comprehensive framework can be burdensome, particularly for small and medium-sized enterprises (SMEs) with limited resources. Compliance costs, including legal advice, staff training, and implementation of technical measures, can place a considerable financial strain on organisations.

Ambiguity and Interpretation Issues. The GDPR's provisions are often open to interpretation, leading to ambiguity and uncertainty. This ambiguity can create challenges for organisations seeking to comply with the regulation. The lack of clear guidelines on certain aspects, such as consent requirements or the application of legitimate interests, can result in inconsistent interpretations and difficulties in determining the appropriate course of action. This situation may lead to legal uncertainties and disputes[9].

Extraterritorial Reach and Global Compliance. The extraterritorial reach of the GDPR presents challenges for organisations operating outside the EU. Non-EU businesses that process personal data of EU residents must comply with the GDPR if they offer goods or services to EU individuals or monitor their behaviour. This global impact raises compliance challenges for organisations outside the EU, as they may need to navigate conflicting or overlapping data protection laws across different authorities.

Impacts on Innovation and Technological Advancements

The GDPR›s strict requirements, particularly regarding consent and data minimisation, can potentially hinder innovation and technological advancements. Start-ups and organisations that heavily rely on data processing for product development and improvement may face challenges in achieving a balance between privacy compliance and innovation. The need for explicit consent and limitations on data use may limit the scope of research and development activities.

Burden on Data Protection Authorities. The GDPR places significant responsibilities on data protection authorities (DPAs) to enforce the regulation effectively. However, DPAs face challenges due to limited resources and capacity constraints. The increased workload of handling data breach notifications, conducting investigations, and ensuring compliance for a vast number of organisations can strain the resources of DPAs. This may lead to delays in resolving complaints and enforcing the regulation consistently.

Impact on Cross-Border Data Transfers. The GDPR introduces strict requirements for transferring personal data to countries outside the EU deemed as lacking adequate data protection standards. This impacts international data transfers, particularly between EU and non-EU countries. Organisations may face challenges in ensuring

[9] www.mckinsey.com. (n.d.). GDPR compliance challenges since May 2018 | McKinsey. [online] Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge.

compliance with these requirements, such as implementing appropriate safeguards or relying on legal mechanisms, potentially disrupting global business operations.

Impact on Digital Marketing and Advertising Practices. The GDPR's provisions on consent and the right to object have had a significant impact on digital marketing and advertising practices. Organisations face challenges in obtaining valid and freely given consent, particularly in the context of online tracking, profiling, and targeted advertising. The shift toward more transparent and privacy-friendly practices can disrupt traditional advertising models and require organisations to find innovative ways to engage with consumers[10].

Risks of Over-Compliance and Data Protection Fatigue. The GDPR's strict requirements, combined with potential severe penalties for non-compliance, may lead to a culture of over-compliance. Organisations may implement excessively cautious measures to avoid any potential risk, resulting in a conservative approach to data processing. Moreover, individuals may experience «data protection fatigue» due to the overwhelming number of privacy notices and consent requests, potentially leading to reduced engagement and undermining the intended benefits of the GDPR.

While the GDPR represents a crucial step towards enhancing data protection and privacy, it is important to recognize the challenges and potential downsides associated with its implementation. The complexity of the regulation, compliance burdens, ambiguity, and interpretation issues can pose significant challenges for organisations. Additionally, the GDPR›s global impact, impacts on innovation, burden on DPAs, cross-border data transfers, and effects on digital marketing practices require careful consideration. Addressing these challenges and striking a balance between privacy protection and practical implementation will be essential for maximizing the benefits of the GDPR while minimizing potential negative consequences.

Directives Developments Outside the EU. While the European Union (EU) has undoubtedly taken a significant step in data protection by implementing the General Data Protection Regulation (GDPR), it is crucial to recognize that numerous other authorities worldwide are also grappling with the challenges presented by modern technology in the realm of privacy and data protection. In response to these challenges, many countries have either already introduced or are in the process of enacting their own data protection laws. The scope and nature of these laws vary from one jurisdiction to another, resulting in a patchwork of data protection compliance obligations for businesses operating across different regions.

This regulatory fragmentation poses a considerable burden on multinational companies, as they must navigate through a complex web of legal requirements, often with conflicting provisions. The influence of the GDPR on global data protection laws cannot be overlooked. In certain cases, the GDPR has served as a catalyst for legislative changes in countries that have achieved adequacy decisions from the European Commission. Adequacy decisions, which permit the transfer of personal data from the EU to those jurisdictions without additional safeguards, come with a limited duration. Consequently, these authorities have updated their domestic data protection laws to

[10]Andrada Coos (2018). GDPR: The Pros and The Cons. [online] Endpoint Protector Blog. Available at: https://www.endpointprotector.com/blog/gdpr-the-pros-and-the-cons/.

align them more closely with the principles and standards set forth in the GDPR.

For instance, Japan, which had obtained an adequacy decision from the European Commission in 2019, recognised the need to revise its Act on the Protection of Personal Information (APPI) to ensure ongoing alignment with the GDPR. APPI is a comprehensive legislation enacted in 2003 to ensure the privacy and data protection rights of individuals in Japan. In 2020, the APPI underwent significant amendments to align with global privacy standards, particularly the European Union›s General Data Protection Regulation (GDPR).

The APPI's Scope and Application:

The APPI applies to both public and private entities operating in Japan, encompassing a wide range of personal information. It covers identifiable data such as names, addresses, and social security numbers, aiming to protect individuals› sensitive data from misuse or unauthorised access.

Fundamental Principles:

Built on the principles of legality, fairness, and transparency, the APPI emphasizes obtaining consent from individuals for the collection, use, and disclosure of their personal data. It establishes a framework that promotes responsible data managing practices, ensuring that individuals are informed about the purpose and extent of data processing[11].

Data Subject Rights:

The APPI grants individuals several rights regarding their personal information. These rights include the ability to access and correct their data, request the suspension of data use or disclosure, and, under certain circumstances, request the deletion of their personal information. By empowering individuals with these rights, the APPI reinforces their control over their own data.

Cross-Border Data Transfers:

To safeguard personal data when transferring it to third countries, the APPI imposes restrictions and requires entities to ensure an adequate level of protection. This aligns with international data transfer standards and emphasizes the importance of maintaining data security and privacy, even beyond Japan›s borders.

Security Measures and Breach Notification:

Entities subject to the APPI must implement appropriate security measures to protect personal data from unauthorized access, loss, alteration, or disclosure. Regular risk assessments and the development of internal data protection policies are essential components of this process. In the event of a personal data breach, entities are required to promptly notify affected individuals and relevant authorities, taking necessary measures to mitigate risks and prevent future breaches.

Data Protection Authorities and Penalties:

The APPI establishes the Personal Information Protection Commission (PPC) as the regulatory authority responsible for overseeing compliance with the APPI. The PPC holds the power to conduct inspections, issue administrative orders, and impose penalties for non-compliance. The amended APPI introduced stricter penalties, includ-

[11]Japan updates enforcement rules for amended APPI. [online] Available at: https://iapp.org/news/a/japan-updates-enforcement-rules-for-amended-appi/.

ing increased fines, to ensure effective enforcement and incentivize adherence to data protection practices. Japan›s Act on the Protection of Personal Information (APPI) serves as a crucial framework for safeguarding privacy in the digital era. With its comprehensive provisions, alignment with global privacy standards, and emphasis on individual rights and consent, the APPI reinforces Japan›s commitment to protecting personal data. By establishing clear guidelines, promoting responsible data handling practices, and imposing penalties for non-compliance, the APPI aims to strike a balance between facilitating data-driven innovation and preserving individuals› privacy rights. As technology continues to advance, the APPI serves as a significant legislative instrument in ensuring the protection of personal information in Japan[12]. Similarly, the Republic of Korea witnessed significant updates to its Personal Information Protection Act (PIPA). The PIPA in Korea is a comprehensive legislation designed to regulate the collection, use, and disclosure of personal information. Enacted in 2011, the PIPA applies to both public and private entities and sets forth principles and guidelines for responsible data handling.

The law emphasizes the importance of informed consent, purpose limitation, and data security. It grants individuals various rights, including the right to access their personal information, request corrections, and withdraw consent. The PIPA also imposes obligations on data handlers, such as implementing safeguards, conducting risk assessments, and notifying individuals and authorities in case of data breaches. The Personal Information Protection Commission (PIPC) is responsible for enforcement, ensuring compliance, and imposing penalties for violations of the PIPA[13].

Korea's PIPA is a robust legal framework that safeguards personal information and promotes privacy rights. It establishes principles and requirements for the proper handling of data, grants individuals' control over their personal information, and outlines obligations for organisations that oversee personal data. With the PIPA in place, Korea aims to ensure the protection of personal information, enhance data security measures, and maintain a responsible data protection environment in the country[14]. The National Assembly of the Republic of Korea approved several updates on the act on 4th of February 2020, and they came into force in August 2020. These reforms played a pivotal role in the European Commission›s decision to adopt an adequacy decision for the Republic of Korea on 17 December 2021. The European Commission acknowledged the reform of PIPA as a significant step in the adequacy talks, contributing to the favourable outcome[15].The aim for these countries is to ensure that their local data protection laws sufficiently align with the GDPR to avoid disruptions in the free flow of data when their adequacy decisions undergo review.

By incorporating GDPR-aligned provisions into their national legislation, these authorities aim to demonstrate their commitment to data protection and establish a

[12] www.japaneselawtranslation.go.jp. (n.d.). Act on the Protection of Personal Information - English - Japanese Law Translation. [online] Available at: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en.
[13] www.linklaters.com. (n.d.). Data Protected Republic of Korea| Insights | Linklaters. [online] Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---republic-of-korea.
[14]Wall, A. (2018). GDPR matchup: South Korea's Personal Information Protection Act. [online] Iapp.org. Available at: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.
[15] Wall, A. (2018). GDPR matchup: South Korea's Personal Information Protection Act. [online] Iapp.org. Available at: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.

level of harmonization with the EU›s robust privacy framework. However, despite these efforts, achieving complete harmonization across all aspects of data protection laws remains a challenge. Authorities must strike a delicate balance between safeguarding individuals› privacy rights and fostering innovation and economic growth. Moreover, the GDPR itself is a complex regulation, and aligning with its provisions requires careful consideration and adaptation to local contexts.

Brexit's impact on the country's alignment with GDPR

In the following section, we will examine the implications of the United Kingdom›s exit from the European Union on personal data protection regulations. The withdrawal of the United Kingdom from the EU, commonly known as Brexit, has brought significant changes to the data protection landscape in the UK. Prior to Brexit, the General Data Protection Regulation (GDPR) was directly applicable in the UK as it is in all EU member states.

The withdrawal of the United Kingdom (UK) from the EU, has affected the GDPR in several ways. Since 1 January 2021, the UK is no longer part of the EU or the EEA, which means that it is considered a third country for data transfers from and to the EU or the EEA. The UK has also adopted its own version of the GDPR, which is like the EU regulation, but with some differences and potential divergences in the future.

The EU has granted an adequacy decision to the UK, which allows personal data to flow freely from the EU and EEA to the UK without any additional safeguards. However, this adequacy decision is subject to review and suspension or revocation if the EU finds that the UK›s data protection regime does not ensure an adequate level of protection.

The following paragraphs aim to provide an overview of Brexit›s impact on GDPR, and to highlight some of the main challenges and opportunities for organisations and individuals in relation to data protection and privacy.

- The UK has adopted its own version of the GDPR: The UK has enacted the GDPR›s requirements into UK law, forming a new, UK-specific data protection regime that works after Brexit. The UK›s post-Brexit version of the GDPR is like the EU regulation, so there is slight change to the data protection principles and obligations. However, there are some differences, such as the UK›s ability to make its own adequacy decisions for data transfers to third countries, or to diverge from the EU›s interpretation or application of the GDPR in the future.
- The UK has been recognized as ‹adequate› by the EU: The EU has granted an adequacy decision to the UK, which means that personal data can flow freely from the EU and EEA to the UK without any additional safeguards. The adequacy decision is valid for four years and can be renewed if the EU considers that the UK continues to ensure an adequate level of data protection. However, the adequacy decision can also be suspended or revoked if the EU finds that the UK›s data protection regime diverges significantly from the EU›s standards or infringes on individuals› rights.
- The UK is a third country for data transfers from the UK to the EU: The UK is no longer part of the EU or the EEA, which means that it is considered a third country for data transfers from the UK to the EU or the EEA. This means that UK organisations that transfer personal data to the EU or the EEA must comply with the rules and obligations under the GDPR for such transfers, such as ensur-

ing an adequate level of protection, providing appropriate safeguards, or relying on derogations.

- The UK and the EU have separate data protection authorities and regimes: The UK is no longer subject to the authority or supervision of the EU›s data protection authorities or the European Data Protection Board. The UK has its own data protection authority, the Information Commissioner›s Office (ICO), which is responsible for enforcing the UK›s data protection regime and issuing guidance and recommendations. The UK and the EU have separate data protection regimes, which means that organisations that operate in both authorities may have to comply with different rules and obligations or face different sanctions and remedies for non-compliance or infringement[16].
- The UK and the EU may require data protection representatives: The UK and the EU have extra-territorial effect, which means that they apply to organisations that are not established in their respective jurisdictions, but that offer goods or services to individuals in their jurisdictions or monitor their behaviour. Such organisations may be required to appoint data protection representatives in the UK or the EU, respectively, to function as a point of contact for individuals and data protection authorities, and to cooperate with them on any issues related to the processing.

Brexit has had a significant impact on GDPR, creating a new, UK-specific data protection regime that works alongside the EU regulation. The UK has been recognised as ‹adequate› by the EU, allowing personal data to flow freely from the EU and EEA to the UK without any additional safeguards. However, this adequacy decision is subject to review and suspension or revocation if the EU finds that the UK›s data protection regime does not ensure an adequate level of protection. The UK is also a third country for data transfers from the UK to the EU or the EEA, which means that UK organisations that transfer personal data to the EU or the EEA must comply with the rules and obligations under the GDPR for such transfers. The UK and the EU have separate data protection authorities and regimes, which means that organisations that operate in both authorities may have to comply with different rules and obligations or face different sanctions and remedies for non-compliance or infringement.

The UK and the EU may also require data protection representatives for organisations that are not established in their respective authorities, but that offer goods or services to individuals in their jurisdictions or monitor their behaviour. Brexit poses many challenges and opportunities for organisations and individuals in relation to data protection and privacy[17].

It is essential for organisations and individuals to understand and comply with the GDPR and the UK GDPR, and to adopt an initiative-taking and responsible approach to data protection and privacy. It is also important for organisations and individuals to seek advice and guidance from experts on data protection and privacy matters, and to consult with individuals and stakeholders on their data processing activities. By doing so, organisations and individuals can ensure that they respect the rights and interests

[16]ICO (2023a). The research provisions. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/.

[17]ICO (2023). UK GDPR guidance and resources. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

of individuals in relation to their personal data, and benefit from the opportunities that data protection and privacy offer[18].

In conclusion, the General Data Protection Regulation (GDPR) has emerged as a crucial framework in safeguarding individuals' privacy rights and shaping data protection regulations worldwide. Its impact extends far beyond the European Union, serving as a catalyst for the development of similar legislation in other countries. The GDPR's emphasis on transparency, consent, and accountability has inspired nations to re-evaluate their own data protection practices and enact comprehensive regulations to ensure the responsible handling of personal information. By promoting a global standard for data privacy, the GDPR has ignited a transformative shift in the way organizations collect, process, and store data, ultimately empowering individuals and fostering a culture of data privacy and security across borders. As the digital landscape continues to evolve, the influence of GDPR serves as a reminder of the vital importance of robust data protection measures and the collective responsibility to safeguard individuals' sensitive information in an increasingly interconnected world.

BIBLIOGRAPHY

1. eur-lex.europa.eu. (n.d.). Directive 95/46/EC of the European Parliament and of the Cou... - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:31995L0046.
2. eur-lex.europa.eu. (n.d.). EUR-Lex - 32002L0058 - EN - EUR-Lex. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.
3. Legislation.gov.uk. (2020). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. [online] Available at: https://www.legislation.gov.uk/eudr/2006/24/contents.
4. Legislation.gov.uk. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). [online] Available at: https://www.legislation.gov.uk/eur/2016/679/contents.
5. digital-strategy.ec.europa.eu. (n.d.). ePrivacy Regulation | Shaping Europe's digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.
6. Custers, B., Van der Hof, S., Schermer, B. (2014) Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies, Policy & Internet, Vol. 6, No. 3, pp. 268–295.
7. Custers, B.H.M., and Bachlechner, D. (2018) Advancing the EU Data Economy; Conditions for Realizing the Full Potential of Data Reuse, Information Polity, https://doi.org/10.3233/ip170419.

[18]ICO (2023). UK GDPR guidance and resources. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

8. GDPR (2018). General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.
9. GDPR (2018). General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.
10. www.mckinsey.com. (n.d.). GDPR compliance challenges since May 2018 | McKinsey. [online] Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge.
11. Andrada Coos (2018). GDPR: The Pros and The Cons. [online] Endpoint Protector Blog. Available at: https://www.endpointprotector.com/blog/gdpr-the-pros-and-the-cons/.
12. Japan updates enforcement rules for amended APPI. [online] Available at: https://iapp.org/news/a/japan-updates-enforcement-rules-for-amended-appi/.
13. www.japaneselawtranslation.go.jp. (n.d.). Act on the Protection of Personal Information - English - Japanese Law Translation. [online] Available at: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en.
14. www.linklaters.com. (n.d.). Data Protected Republic of Korea| Insights | Linklaters. [online] Available at: https://www.linklaters.com/en/insights/data-protected/data-protected---republic-of-korea.
15. Wall, A. (2018). GDPR matchup: South Korea's Personal Information Protection Act. [online] Iapp.org. Available at: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.
16. Wall, A. (2018). GDPR matchup: South Korea's Personal Information Protection Act. [online] Iapp.org. Available at: https://iapp.org/news/a/gdpr-matchup-south-koreas-personal-information-protection-act/.
17. ICO (2023a). The research provisions. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/.
18. ICO (2023). UK GDPR guidance and resources. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.
19. Christopher Kuner and others, The global data protection implications of 'Brexit', International Data Privacy Law, Volume 6, Issue 3, August 2016, Pages 167–169, https://doi.org/10.1093/idpl/ipw018