Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 16 (1), 2024
pp. 787 - 794

# Balancing Between Fiscal Interests and Privacy Data Protection

**[1]Gunawan Widjaja***
[1]Faculty of Law, Universitas 17 Agustus 1945 Jakarta, Indonesia
*email: widjaja_gunawan@yahoo.com
https://orcid.org/0000-0002-1558-362X

**Abstract:** The digital era presents new challenges and opportunities in personal data management, demanding dynamic and responsive adaptation of public policies to balance technological innovation, individual privacy, and economic interests. The results of this study show that the implementation of data protection policies in tax law has the potential to increase public trust in the tax system significantly. This promising finding suggests that policies that ensure personal data protection are consistently integrated into tax procedures can encourage higher tax compliance. Moreover, the adoption of technology, such as cloud computing and blockchain, plays a pivotal role in corporate governance, improving data protection and offering operational efficiency. This emphasis on the role of technology reassures the audience about the potential benefits of technological adoption. Furthermore, tax agencies that regularly evaluate and update their policies to align with the latest technological developments and changing privacy norms show higher public trust. This confirms that active engagement of tax agencies in discussions on the ethics of data processing and artificial intelligence can strengthen transparency and accountability. Therefore, a combination of legal reforms, investments in security technologies, and a dynamic and inclusive regulatory approach are key factors in creating a tax system that is efficient and ethical, in line with modern society's expectations for privacy and data management.

**Keywords:** Tax Law, Privacy Policy, Fiscal Interests, Data Protection.

**Received:**13 March 2024 **Revised:**19 May 2024 **Accepted:**16 June 2024

## 1. Introduction

In the current era of globalization and the digital revolution, technology's role in every aspect of life, including the tax sector, has become increasingly significant. Technological innovations have not just changed but transformed the way tax institutions collect, process, and store taxpayer data, ushering in unprecedented efficiency and effectiveness. The urgency of tax policy reform has become even more pronounced with the rapid growth of the digital economy that transcends traditional jurisdictional boundaries. The digital transformation has not just created new business models, facilitated easy cross-border transactions, and generated new sources of revenue but also brought to light the inadequacies of conventional tax legal frameworks [1].

This presents significant challenges for governments in ensuring equitable distribution of the tax burden and avoiding tax base erosion. Therefore, tax policy reform is necessary not only to adjust to the dynamics of the digital economy but also to ensure fairness, efficiency of tax collection, and prevention of tax evasion [2]. Tax policy adaptation is crucial to strengthening fiscal infrastructure, responding to changes in the business environment, and ensuring that countries have the ability to finance public needs in the digital era [3]. Tax, as the main instrument of state fiscal policy, has an important role in financing public expenditure and achieving economic stability. To improve the efficiency of tax collection, the use of taxpayer personal data is becoming increasingly intensive [4]. The collection, processing, and storage of personal data by tax

authorities increases the risk of privacy violations if not managed carefully and in accordance with data protection principles [5].

The challenge of data protection in the tax collection process arises from the need to balance tax collection effectiveness and respect for taxpayer privacy. In this digital age, tax authorities collect, process, and store large amounts of personal data to improve tax compliance and minimize tax evasion [6]. However, this presents significant risks to data security and privacy, including leakage of sensitive information, use of data for unauthorized purposes, and unauthorized access by third parties [7]. In addition, applying advanced data collection technologies such as predictive analytics and machine learning raises questions regarding transparency and accountability in data processing. These challenges require tax authorities to align their practices with strict data protection principles and build trust with the public, ensuring that data collection is conducted ethically and securely [8].

On the other hand, the importance of personal data protection has been recognized globally, as reflected in various international regulations and initiatives, including the General Data Protection Regulation (GDPR) in the European Union. Protecting individuals' personal information is not only an ethical obligation but also a legal one, given the consequences of data breaches for individuals and institutions [4]. However, in practice, there is a tendency for conflict between fiscal interests and the right to privacy. On the one hand, governments and tax authorities must ensure the efficiency and effectiveness of tax collection for public financing. On the other hand, they must also comply with data protection principles and regulations to safeguard taxpayers' privacy. Finding a balance between these two interests is a complex challenge [9].

Data breach cases in recent years demonstrate the significant risks of inadequately protected data collection practices, fuelling public concerns about privacy risks and questioning the integrity of tax collection systems [10]. Therefore, it is important to explore how tax law and privacy policy can adapt and evolve to accommodate both aspects, ensuring that fiscal interests can be met without compromising personal data protection.

This research aims to fill the gap in the literature by analyzing the interaction between tax law and privacy policy, identifying existing challenges, and proposing ways to balance fiscal interests with data protection. By understanding the limitations and potential solutions, it is possible to formulate a policy framework that enables efficient tax collection while ensuring high data protection for individuals.

## 2. Methodology

The study conducted in this research uses the literature research method. The literature research method is used in academic research to collect and analyze relevant information on a particular topic from secondary text sources, such as journals, books, and online articles. Researchers use this method to identify, collate, and analyze various data sources related to the topic under study, which helps build a theoretical or conceptual framework for their research. This process includes searching for relevant keywords in various databases and catalogs to find appropriate literature, followed by evaluating the eligibility and relevance of the sources to the research objectives [11] [12] [13].

## 3. Discussion

### *3.1. Tax Law*

The principles of tax law are the philosophical and theoretical foundations that form the basis for developing and applying tax regulations in various jurisdictions. These principles include fairness, efficiency, certainty, convenience, economy, and flexibility. Fairness in taxation is divided into horizontal fairness, where individuals of equal economic means are taxed equally, and vertical fairness, where individuals of greater economic means pay more [14]. Efficiency refers to a tax system designed to collect revenue with minimal impact on economic decisions. Certainty ensures taxpayers understand when, how, and how much tax to pay. Convenience emphasizes a tax system that is easy for taxpayers and tax authorities to understand and administer. The economic principle refers to the cost of collecting taxes that should be minimal. Finally, the flexibility of tax principles allows the tax system to adapt to changing economic and social conditions [15].

The evolution of tax law in the digital age is characterized by the rapid development of technology that forces tax authorities and legislators worldwide to adopt tax law frameworks to remain relevant to new business models and emerging ways of economic transactions. An increasingly connected world and the dominance of the digital economy, including electronic commerce, the sharing economy, and cryptocurrencies, challenge conservative principles of taxation, particularly concerning issues of location of economic activity and determination of the place of tax collection [16]. Responses to these changes include the implementation of BEPS (Base Erosion and Profit Shifting) by the OECD, which aims to address tax avoidance by multinational corporations, as well as the introduction of digital taxes to capture the value generated by large digital companies in countries where they do not have a significant physical presence [17]. Artificial intelligence and blockchain technology are also utilized to improve tax compliance and administrative efficiency. These transformations represent a vital transition in tax law, blending old principles with new realities to create a fair and efficient system in a changing global economic environment [18].

Therefore, the evolution of tax law in the digital age is a response to the economic transformation brought about by technology. This includes adapting tax regulations to address challenges arising from the digital economy, such as profit shifting, electronic commerce, and business entities without physical form. Global initiatives such as BEPS by the OECD and the implementation of digital taxation demonstrate international efforts in creating a fairer, more effective, and digital-appropriate tax system. New technologies such as AI and blockchain are projected to improve tax administration, reduce tax evasion, and facilitate tax compliance. This signifies an important shift from traditional tax principles to innovative practices, ensuring the global tax system remains relevant and effective amid economic and technological developments.

### *3.2. Personal Data Protection*

The general principles of data protection, which are the backbone of regulations such as the General Data Protection Regulation (GDPR) in the European Union and similar regulations worldwide, include several core rules. First, the principle of lawful, fair, and transparent processing requires that personal data be collected and processed lawfully, fairly, and transparently to the subject of data [19]. Furthermore, the principle of limitation of purpose stipulates that data should only be collected for specific, explicit, and legitimate purposes, and data minimization ensures that only data that is truly necessary for the purpose is collected. The principle of accuracy encourages the accuracy of information, while storage limitation stipulates that personal data should be kept for a period no longer than necessary [20]. Integrity and confidentiality underscore the importance of safeguarding data from unauthorized access or illegal processing. Finally, the principle of accountability requires data controllers to be responsible and able to demonstrate compliance with all of these principles, cementing data protection as an important ethos in the policies and practices of an organization or corporation [21].

Data protection regulations worldwide have significantly developed in recent years in response to growing privacy and data protection concerns. One of the most important and influential examples is the General Data Protection Regulation (GDPR) enacted by the European Union in May 2018 [22]. GDPR has set new data protection and privacy standards, not only for entities operating within the European Union but also for companies around the world that process the data of EU citizens. The regulation implements the principles of more significant consent, transparency, and control for data subjects over their personal data and substantial penalties for organizations that violate them. The GDPR also encourages the implementation of Privacy by Design, which integrates data protection and privacy into every stage of product or service development [23].

Outside of Europe, many countries have developed or updated their own data protection regulations, inspired by the GDPR or as independent initiatives to improve the protection of their citizens' privacy rights. For example, the California Consumer Privacy Act (CCPA) in the United States, which came into effect in January 2020, gives California consumers new rights, including the right to know what information is being collected about them by businesses and the right to request the deletion of that data [24]. In Asia, the Personal Data Protection Acts passed by Singapore and Japan underscore the importance of protecting

personal data and establishing a framework for fair and lawful data use and collection. Globally, frameworks such as the GDPR have become models for many countries in drafting or modifying their data protection regulations, confirming the global trend toward stronger privacy and data protection [25].

### *3.3. The Tax and Privacy Dilemma*

Privacy breaches are a significant risk in tax data collection, especially as tax authorities collect and process large volumes of taxpayer personal and financial data. As the tax administration militarises, the risk of data leakage, theft, or misuse increases, whether due to cyber-attacks or lapses in system security. Privacy concerns are also exacerbated by the potential use of tax data beyond the initially collected purpose, including unauthorized monitoring or profiling [26]. Therefore, strengthening policies and security mechanisms to protect personal information in the tax system is essential to maintain public trust and meet increasingly stringent data protection legal standards in many jurisdictions. The inability to manage these risks can result in large financial losses, reputational damage, and disruption to tax compliance [27].

The conflict between the government's fiscal interests and the right to individual privacy is often a hot spot in discussing tax policy regulation and implementation. On the one hand, governments have a fiscal interest in collecting taxes effectively and efficiently to fund public programs and social services [28]. This often requires collecting detailed personal and financial data from individuals and businesses to ensure tax compliance and identify tax evasion. However, collecting, using, and storing this data can potentially touch the boundaries of privacy guaranteed by law or social norms, especially if sensitive data is managed without adequate care or transparency [29].

In contrast, the right to privacy is a fundamental principle recognized by many global data protection regulations, such as the GDPR, which demands that any collection and processing of personal data must be done in a lawful, fair, and transparent manner. The need to strengthen privacy often conflicts with the logic of broad and deep fiscal oversight [30]. This conflict creates the challenge of designing a tax system that is not only effective from a fiscal standpoint but also respects taxpayers' privacy. Harmonization between these two interests requires ongoing dialogue, effective oversight, and the implementation of technologies capable of protecting personal data while providing tax authorities the necessary access to fulfill their duties [31]. Without careful balancing, the potential for conflicts of interest to escalate remains a real risk, emphasizing the importance of transparency and accountability in all aspects of tax administration [32].

### *3.4. Strategy for Balancing Interests*

Implementing the principle of data minimization in tax collection demands that tax authorities only collect data strictly necessary for taxation without going overboard. This means that personal and financial information collected from taxpayers should be limited to what is needed for assessing tax liabilities, auditing and checking compliance, and other tax administration services [33]. The application of this principle aims to reduce privacy-related risks and strengthen public trust in the tax system by ensuring that data collection and processing are conducted in a way that respects individuals' privacy rights and minimizes the potential for data misuse [34]. Despite its importance, implementing data minimization in tax collection faces challenges, including balancing the need for fiscal transparency with privacy protections and ensuring that restrictions on the data collected do not hinder the ability of tax authorities to carry out their duties effectively [35].

In continuing data minimization practices, tax authorities face the challenge of navigating the evolving technology and big data environment. Implementing advanced technologies such as big data processing and artificial intelligence offers the potential to improve the efficiency and effectiveness of tax collection but also increases risks to privacy if their use is not carefully regulated [36]. It is, therefore, important for tax authorities to adopt an approach that considers privacy from design, ensuring that technological systems and processes used for tax collection are designed to include data protection considerations from the outset. This also involves continuous education and awareness for tax authority employees on the importance of data minimization and privacy protection and the development of clear policies on data access, use, and storage [37]. These strategies can help ensure that the collection and management of tax data is not only efficient from an administrative point of view but also complies with the highest standards

of privacy protection, reducing the risk of intrusion into taxpayers' privacy and strengthening legitimacy and trust in the tax system [38].

The application of encryption technology in data security is an important step taken by various entities, including government agencies, companies, and organizations, to protect sensitive and personal information from unauthorized access. Encryption technology converts readable information into encrypted data (cipher text) that can only be accessed or converted back into its original form by individuals who possess the appropriate decryption key [39]. This method effectively maintains data confidentiality when stored on hardware or transmitted over insecure networks like the internet. Using layered encryption and strong encryption standards, such as AES (Advanced Encryption Standard) and RSA, adds an important layer of protection that makes data more resistant to eavesdropping attempts, identity theft, and other forms of cyberattacks [40].

In addition to encryption technologies, implementing a comprehensive data security policy often involves other strategies such as multi-factor authentication, strict access management, and continuous network monitoring. Multi-factor authentication ensures that access to sensitive data is restricted to verified users through multiple verification methods, such as a combination of passwords, security codes sent via SMS, or fingerprints [41]. Strict access management establishes role-based access rights, where individuals are only granted access to information relevant to their tasks. Continuous network monitoring helps identify and manage potential security threats in real-time. Together, these techniques and strategies form a robust security framework, reducing the likelihood of data breaches and ensuring that sensitive information is protected to high privacy and security standards [42].

In conclusion, using encryption technology and implementing data security through various important strategies are essential in protecting sensitive and personal information from cyber threats and attacks in today's digital age. Encryption technology provides a strong layer of protection by ensuring that data, whether stored or in the transmission process, can only be accessed by individuals with the appropriate decryption key. Additional data security strategies, such as multi-factor authentication, strict access management, and continuous network monitoring, further strengthen the information security system by restricting unauthorized access and monitoring suspicious activity.

Implementing and maintaining these security mechanisms not only meets the data protection needs from a technical aspect but also builds trust and reliability in the digital environment for individuals and organizations. In an increasingly connected and data-dependent global context, security and privacy are no longer just a practical necessity but have become an ethical responsibility for all parties involved in data management [43]. Therefore, it is important for every entity, including governments, companies, and other organizations, to proactively adopt and update their data security policies in accordance with the latest security standards to protect the privacy rights of individuals and ensure the integrity and security of digital information.

In designing policies that accommodate fiscal needs while maintaining strong data protection, policymakers should consider balancing cost efficiency and investment in security infrastructure. Policies should formulate ways for efficient budget allocation that strengthens data security systems without overspending resources [44]. This can be achieved by a detailed risk assessment, where resources are allocated based on the urgency and importance of the protected data assets. Thus, the allocation of funds can be targeted towards the most critical aspects of data protection, such as end-to-end encryption and multi-layered security systems, while avoiding unnecessary spending on less critical components [45].

Another strategy that can be adopted in this policy is cooperation and partnership with the private sector to develop more effective and lower-cost data security solutions. Utilizing new technologies, such as cloud computing, can reduce local infrastructure costs while increasing the robustness and scalability of data security systems [46]. This cooperation could also involve cost-sharing schemes or outcome-based payment models, where governments can access the latest data security technologies without bearing all the initial development and implementation costs [47].

Finally, the policy should include clear guidelines on data governance, emphasizing that any use or management of data by government entities should always adhere to high-security standards, no matter how large or small the expenditure required. This includes establishing transparent data usage rules,

regular auditing processes, and returning information to users in case of a data breach [48]. Governments can maintain public trust while optimizing fiscal expenditure by integrating preventive and reactive measures against data security incidents into the fiscal framework [49].

## 4. Conclusions

Fiscal interests and data protection are often in conflict. On the one hand, the need for efficiency and savings in budget management pushes governments and organizations to limit spending, including data security. Meanwhile, the demand for high data protection necessitates significant investment in information security technology and IT infrastructure, which often requires large expenditures. To resolve this contradiction, the use of the right technology is key. Solutions such as cloud computing, end-to-end encryption, and blockchain technology offer ways to enhance data security while potentially reducing traditional IT infrastructure's operational and maintenance costs, providing a pathway to strike a balance between fiscal and data protection aspects.

Adopting the right policies also plays a crucial role in achieving this balance. For example, policies that allow for strategic cooperation with the private sector can open up access to data security technology innovations while sharing the cost burden. In addition, regulations that encourage or even require using specific security standards in data management by public and private entities can raise the bar of data security without automatically requiring a large increase in budget allocations. Thus, through wise technology choices and policies that support collaboration and standardization, fiscal interests and data protection can coexist and reinforce each other to achieve a safer and more efficient common goal.

Tax law reforms incorporating data protection aspects are becoming increasingly important, especially in this digital age, where the volume and sensitivity of information handled by tax authorities have significantly increased. The explicit integration of data protection policies in tax regulations will ensure that all personal data collected, processed, and stored by tax agencies are protected according to high-security standards. This will not only strengthen public confidence in a fair and secure tax system but also reduce the risk of data breaches that could affect the credibility and efficiency of the tax system as a whole. The implementation of these reforms requires inter-sectoral cooperation and regulatory adjustments that are transparent and inclusive, ensuring ethical and responsible data management in all tax operations.

## References


[1] Amankwah, J., & Schoubroeck, C. V. (2022). Fraud detection in motor insurance: Privacy and data protection concerns under EU Law. *International Data Privacy Law*, *12*(3), 220–238. https://doi.org/10.1093/idpl/ipac009

[2] Bagheri, P., & Althabhawi, N. M. (2022). Islamic and European Perspectives on Data Privacy in Online Contracts. *European Data Protection Law Review*, *8*(3), 377–385. https://doi.org/10.21552/edpl/2022/3/7

[3] Bartlett, M. (2021). Beyond Privacy: Protecting Data Interests in the Age of Artificial Intelligence. *Law, Technology and Humans*, *3*(1), 96–108. https://doi.org/10.5204/lthj.1595

[4] Cameron, S. (2020). Policy Forum: Independent Platform Costing—Balancing the Interests of the Public and Parties. *Canadian Tax Journal/Revue Fiscale Canadienne*, *68*(2), 491–504. https://doi.org/10.32721/ctj.2020.68.2.pf.cameron

[5] Benedikt, K. (2021). Germany · New Act on Privacy and Electronic Communications. *European Data Protection Law Review*, *7*(2), 254–259. https://doi.org/10.21552/edpl/2021/2/17

[6] Bincoletto, G. (2021). Italy · Italian DPA Balancing Data Protection and Freedom of Expression: Essentiality and Fairness as key principles. *European Data Protection Law Review*, *7*(1), 115–119. https://doi.org/10.21552/edpl/2021/1/15

[7] Brkan, M. (2022). Privacy, data protection and the role of European Courts: Towards judicialisation and constitutionalisation of European privacy and data protection framework. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 274–302. https://doi.org/10.4337/9781786438515.00022

[8] Burri, M. (2023). Cross-border data flows and privacy in global trade law: Has trade trumped data protection? *Oxford Review of Economic Policy*, *39*(1), 85–97. https://doi.org/10.1093/oxrep/grac042

[9] Chiara, P. G. (2021). The Balance Between Security, Privacy and Data Protection in IoT Data Sharing: *European Data Protection Law Review*, *7*(1), 18–30. https://doi.org/10.21552/edpl/2021/1/6

[10] Citron, D. K. (2023). Opinions · The Fight for Intimate Privacy. *European Data Protection Law Review*, *9*(1), 5–8. https://doi.org/10.21552/edpl/2023/1/4

[11] Abdussamad, Z. (2022). *Buku Metode Penelitian Kualitatif*. *Query date: 2024-05-25 20:59:55*. https://doi.org/10.31219/osf.io/juwxn

[12] Adlini, M. N., Dinda, A. H., Yulinda, S., Chotimah, O., & Merliyana, S. J. (2022). Metode Penelitian Kualitatif Studi Pustaka. *Edumaspul: Jurnal Pendidikan*, *6*(1), 974–980. https://doi.org/10.33487/edumaspul.v6i1.3394
[13] Kim, K., Lee, K., & Kwon, O. (2024). A systematic literature review of the empirical studies on STEAM education in Korea: 2011–2019. *Disciplinary and Interdisciplinary Education in …*, *Query date: 2024-05-10 07:14:07*. https://doi.org/10.1007/978-3-031-52924-5_6
[14] Clifford, D. (2022). Data protection and consumer protection: The empowerment of the citizen-consumer. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 229–248. https://doi.org/10.4337/9781786438515.00019
[15] DeBrabander, F. (2021). Privacy, Character, and Community. *European Data Protection Law Review*, *7*(1), 11–17. https://doi.org/10.21552/edpl/2021/1/5
[16] Deineko, D. (2023). Legal Analysis Of Human Rights` Protection In Asean: Balancing Economic Interests, Humanity And Governance. *KELM (Knowledge, Education, Law, Management)*, *5*, 165–173. https://doi.org/10.51647/kelm.2023.5.28
[17] Dimitrova, D. (2022). Surveillance at the borders: Travellers and their data protection rights. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 303–334. https://doi.org/10.4337/9781786438515.00023
[18] Dix, A. (2023). Two Necessary Approaches to a Privacy-Friendly 2033. *European Data Protection Law Review*, *9*(3), 305–310. https://doi.org/10.21552/edpl/2023/3/7
[19] Dixit, P., & Sharma, S. (2023). Balancing Privacy and Competition: Evaluating the Competitive Effects of India's Data Protection Bill. *Statute Law Review*, *44*(2). https://doi.org/10.1093/slr/hmad004
[20] Dubois, J. (2024). Balancing National Security Interests With Privacy, The Charter And Rule Of Law: Building Checklists Into Operation Planning. *The Journal of Intelligence, Conflict, and Warfare*, *6*(3), 255–257. https://doi.org/10.21810/jicw.v6i3.6409
[21] Elk, M. van. (2024). Opinions · Privacy in Early Modern England. *European Data Protection Law Review*, *10*(1), 14–16. https://doi.org/10.21552/edpl/2024/1/5
[22] Eskhita, R., Manda, V. K., & Hlali, A. (2021). Dubai and Barcelona as Smart Cities: Some Reflections on Data Protection Law and Privacy. *Environmental Policy and Law*, *51*(6), 403–407. https://doi.org/10.3233/epl-210023
[23] Ferrari, V. (2020). Crosshatching Privacy: Financial Intermediaries' Data Practices Between Law Enforcement and Data Economy. *European Data Protection Law Review*, *6*(4), 522–535. https://doi.org/10.21552/edpl/2020/4/8
[24] Frohman, L. (2024). Opinions · Informational Power and the Origins of German Privacy Law. *European Data Protection Law Review*, *10*(1), 9–13. https://doi.org/10.21552/edpl/2024/1/4
[25] Fuster, Gloria González. (2022). Introduction to Research Handbook on Privacy and Data Protection Law. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 1–8. https://doi.org/10.4337/9781786438515.00005
[26] Gerards, J. (2020). Opinions · The Age of Balancing Revisited? *European Data Protection Law Review*, *6*(1), 13–20. https://doi.org/10.21552/edpl/2020/1/5
[27] Gerritsen, J. (2021). The Netherlands · Administrative Court Judgment on the Interpretation of Commercial Interests as Legitimate Interests. *European Data Protection Law Review*, *7*(2), 243–247. https://doi.org/10.21552/edpl/2021/2/15
[28] Gottschalk, T. (2023). European Union · The EU-US Data Privacy Framework (DPF) – A Blueprint for International Data Transfers? *European Data Protection Law Review*, *9*(4), 448–453. https://doi.org/10.21552/edpl/2023/4/11
[29] Grimes, S. M. (2022). The Politics of Children's Privacy. *European Data Protection Law Review*, *8*(1), 14–18. https://doi.org/10.21552/edpl/2022/1/5
[30] Grossman, J. L., & Friedman, L. M. (2023). Opinions · Privacy in Modern American Law and Society. *European Data Protection Law Review*, *9*(2), 98–103. https://doi.org/10.21552/edpl/2023/2/4
[31] Hallinan, D. (2021a). Do We Need Data Protection at All? *Protecting Genetic Privacy in Biobanking through Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 91–128. https://doi.org/10.1093/oso/9780192896476.003.0006
[32] Hallinan, D. (2021b). Genetic Privacy and Other Interests in Biobanking. *Protecting Genetic Privacy in Biobanking through Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 40–66. https://doi.org/10.1093/oso/9780192896476.003.0004
[33] Hallinan, D. (2021c). The Protection of Genetic Privacy in Biobanking at International Level. *Protecting Genetic Privacy in Biobanking through Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 67–90. https://doi.org/10.1093/oso/9780192896476.003.0005
[34] Heuvel, K. van den. (2022). The justiciability of data privacy issues in Europe and the US. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 73–108. https://doi.org/10.4337/9781786438515.00010
[35] Hoepman, J. (2023). Opinions · Privacy Is Hard and Seven Other Myths. *European Data Protection Law Review*, *9*(2), 104–111. https://doi.org/10.21552/edpl/2023/2/5

[36] Horne, D. (2021). Privacy Law: Understanding Data Protection Regulations. *Encyclopedia of Cryptography, Security and Privacy*, *Query date: 2024-06-18 16:32:02*, 1–6. https://doi.org/10.1007/978-3-642-27739-9_1639-1

[37] Huiskers-Stoop, E., Breuer, A., & Nieuweboer, M. (2022). Exchange of Information, Tax Confidentiality, Privacy and Data Protection from an EU Perspective. *Erasmus Law Review*, *15*(2), 86–99. https://doi.org/10.5553/elr.000225

[38] Ismail, S. (2024). Personal Data Protection Policy: Ensuring Effective Implementation Of Data Privacy Policies In Private Higher Institutions. *International Journal of Law, Government and Communication*, *9*(35), 45–55. https://doi.org/10.35631/ijlgc.935005

[39] Kahler, T. (2020). Consent to privacy policy – 'invalid'. *Turning Point in Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 101–104. https://doi.org/10.5771/9783748921561-101

[40] Kukava, K. (2023). Balancing the Right to Privacy and National Security Interests in the Digital Age. *Journal of Law*, *2*. https://doi.org/10.60131/jlaw.2.2023.7711

[41] Leese, M. (2022). Privacy, data protection, and security studies. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 214–228. https://doi.org/10.4337/9781786438515.00018

[42] Malgieri, G. (2022). Automated decision-making and data protection in Europe. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 433–448. https://doi.org/10.4337/9781786438515.00028

[43] Marnau, N. (2022). From law to engineering: A computer science perspective on privacy and data protection. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 197–213. https://doi.org/10.4337/9781786438515.00017

[44] McCullagh, K. (2022). Post-Brexit data protection in the UK - leaving the EU but not EU data protection law behind. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 36–59. https://doi.org/10.4337/9781786438515.00008

[45] Mishra, A. (2024). Fundamental Rights and Data Protection (Balancing Innovation and Privacy in Light of Digital Personal Data Protection Act, 2023). *International Journal of Science and Research (IJSR)*, *13*(5), 332–337. https://doi.org/10.21275/mr24504204804

[46] Miyashita, H. (2022). Data protection laws in Japan. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 128–139. https://doi.org/10.4337/9781786438515.00012

[47] Navarro-Schiappacasse, M.-P., Magasich-Airola, Á.-P., & Jijena-Leiva, R. (2022). Personal data protection: The new paradigm of the tax secret or tax reserve in Chile. *International Data Privacy Law*, *13*(1), 79–91. https://doi.org/10.1093/idpl/ipac020

[48] Ollier-Malaterre, A. (2023). Opinion · Privacy in China: Legal Culture, Literacy, and Imaginaries. *European Data Protection Law Review*, *9*(4), 389–392. https://doi.org/10.21552/edpl/2023/4/4

[49] Penney, J. W. (2022). Canadian privacy law and the post-war freedom of information paradigm. *Research Handbook on Privacy and Data Protection Law*, *Query date: 2024-06-18 16:32:02*, 109–127. https://doi.org/10.4337/9781786438515.00011