IRSHAD Uzbek Journal of Law and Digital Policy |
Volume: 2, Issue: 6
2024

GDPR vs. Weakly Protected Parties in Other Countries

Eshbaev Gayrat Bolibek Ugli
Tashkent State University of Law

Abstract

The General Data Protection Regulation (GDPR) establishes strong privacy rights for EU residents. However, many countries, including the United States, Asia, and Africa, lack similar protections. This creates challenges for multinational corporations and individuals navigating fragmented global data protection frameworks. This study examines the evolution, principles, and extraterritorial effects of GDPR, comparing it with weaker regulatory frameworks globally. Using qualitative and doctrinal research and document analysis, it identifies enforcement gaps, compliance costs, and operational difficulties in cross-border data transfers. Findings emphasize the need for consistent global standards to address the digital divide and ensure fair data practices. Recommendations highlight multilateral cooperation to develop an interoperable and ethical digital ecosystem. While GDPR offers a foundational model, achieving global harmonization requires collective international commitment. The study concludes with actionable suggestions to strengthen global privacy frameworks and protect vulnerable parties in weakly regulated regions.

Keywords: GDPR, Data Protection, Global Standards, Privacy Rights, Compliance, Harmonization, Cross-Border, Digital Divide

APA Citation:

Eshbaev, G. (2024). GDPR vs. Weakly Protected Parties in Other Countries. *Uzbek Journal of Law and Digital Policy*, *2*(6), 55–65. https://doi.org/10.59022/ujldp.254

I. Introduction

Personal data has become one of the most valuable commodities, driving industries and innovations across the world. Social media platforms, e-commerce websites, financial institutions, and government agencies collect, process, and utilize data to enhance their operations (Zelianin, 2022). This explosion of data has brought convenience and economic growth but has also raised fundamental questions about privacy, ownership, and security in the digital space. The European Union's General Data Protection Regulation (GDPR), enforced since May 2018, and has emerged as the global gold standard for data protection. GDPR aims to protect individuals' fundamental rights to privacy while holding organizations accountable for data processing. Its provisions apply not only within the EU but also extraterritorially, making it a global framework.

However, many countries still lack comparable legal safeguards, resulting in a fragmented global regulatory environment (Voigt & von dem Bussche, 2017). For instance, the United States relies on sector-based regulations, while many Asian and African countries have underdeveloped or inconsistently enforced privacy laws. This imbalance creates challenges for multinational corporations and individuals, complicating compliance, legal enforcement, and the protection of privacy rights. Governments also struggle to balance privacy protection with economic growth, technological innovation, and national security concerns.

The lack of global harmonization of privacy laws creates additional risks for individuals and organizations alike (Reis et al., 2024). For individuals, fragmented protections mean unequal access to privacy rights and vulnerability to exploitative practices in regions with weaker safeguards. For corporations, the regulatory imbalance complicates compliance efforts, increases operational costs, and poses significant risks of legal penalties or reputational damage when violations occur. Governments worldwide face a delicate balancing act protecting individual privacy rights while fostering economic growth, encouraging technological innovation, and addressing national security concerns. The tension between these priorities often results in regulatory gaps or enforcement shortcomings.

This article seeks to examine the key differences between the GDPR and less rigorous data privacy frameworks worldwide, focusing on legislative inconsistencies, operational challenges, and ethical dilemmas. Additionally, it underscores the urgent need for international cooperation and harmonization of data protection laws to promote a fair, secure, and trustworthy digital ecosystem. Without global consensus, the vision of a truly equitable and inclusive digital economy remains an elusive ideal.

II. Methodology

This research utilized a document analysis approach to study regulations. The focus was on comparing GDPR and weak protection frameworks in other countries. Official portals were accessed to obtain authentic regulatory texts and policies. The

document analysis approach ensures a structured examination of legal materials and scholarly articles. This method allowed for systematic identification, analysis, and interpretation of relevant data. These terms helped identify literature and frameworks pertinent to the research objectives. Publicly available documents were prioritized to maintain transparency and accessibility. By using widely available sources, we ensured credibility and accountability in the research process. All analyzed materials were cited appropriately in the bibliography.

Primary sources included government portals and official regulatory websites. Secondary sources comprised academic articles, legal commentaries, and policy reviews. To ensure accuracy, we collected data only from verifiable and reliable platforms. These included national and international organizations responsible for data protection laws. The selection of sources was based on relevance to GDPR and comparative frameworks. A rigorous screening process was implemented to exclude out dated or non-authentic materials. The use of keywords guided the search across databases and online libraries. Keywords such as Social Justice and Legal Framework were consistently applied. All sources were evaluated for their credibility and contribution to the research.

The collected data underwent a detailed thematic analysis. Thematic analysis allows the identification of patterns and trends within the legal texts. Key themes like compliance, enforcement, and protection mechanisms were analysed. Comparative analysis between GDPR and weakly protected frameworks was also performed. This involved identifying gaps and strengths in existing regulations. Document analysis further enabled a detailed understanding of regional cooperation in rights and protection. Ethical considerations were maintained by using publicly accessible data. Each source was critically assessed to ensure validity and relevance. Insights were drawn from reliable interpretations of legal frameworks. Bibliographic citations were provided to acknowledge the original sources used.

Ethical research practices were followed throughout the study. Only publicly available data were utilized, ensuring no breach of confidentiality. Proper citations were made for all referenced materials. The document analysis method has inherent limitations, such as reliance on existing data. No empirical data or surveys were conducted, limiting first-hand perspectives. The research heavily depended on the accuracy of public documents and interpretations. Future studies could complement this with interviews or case studies. Despite limitations, the methodology ensured comprehensive insights into GDPR and other frameworks.

III. Results

The comparative study of data protection regulations highlights significant global disparities. By analyzing GDPR alongside U.S., Asian, and African frameworks, the study reveals legal inconsistencies. Primary sources, such as regulatory guidelines, form the foundation of this analysis. Secondary literature and case studies emphasize the practical implications of these regulations. The Facebook-Cambridge Analytica

scandal showcases gaps in U.S. privacy protections (Tarran, 2018). Similarly, the Schrems II decision highlights challenges in EU-U.S. data transfer frameworks. Meanwhile, Google's GDPR fine exemplifies the regulation's strong enforcement mechanisms. These examples underline the need for international collaboration to address regulatory gaps. Harmonized legal standards can ensure equitable privacy protections worldwide. This approach would also support the sustainable development of global digital economies.

The General Data Protection Regulation (GDPR) replaced the 1995 EU Data Protection Directive, addressing challenges posed by rapid technological advancements and the growing frequency and severity of data breaches. The regulation, which became enforceable on May 25, 2018, was designed to create a unified legal framework across European Union member states, ensuring a high standard of personal data protection and addressing the evolving complexities of digital technology and cross-border data flows (Singla, 2024). As technology developed and data processing capabilities expanded, the outdated directive could no longer provide sufficient safeguards against misuse and mishandling of personal data. GDPR's introduction marked a significant shift in data protection law, prioritizing individual rights, organizational accountability, and stringent enforcement measures.

GDPR is based on several core principles that shape its implementation and enforce its objectives. The first principle, lawfulness, fairness, and transparency, requires that data processing activities adhere to legal requirements, are conducted fairly, and are transparent to the individuals whose data is being processed. This ensures that individuals are adequately informed about how their personal data is collected, used, and shared, allowing them to make informed decisions and exercise their rights. This transparency is critical in building trust between organizations and data subjects. The principle of purpose limitation is another cornerstone of GDPR. It mandates that personal data be collected only for specified, explicit, and legitimate purposes and that it not be further processed in a manner incompatible with those purposes (Singh & Prerna, 2024).

The principle ensures that organizations cannot repurpose data arbitrarily, reducing the likelihood of misuse and unauthorized applications. In addition, data minimization requires organizations to limit data collection to what is necessary for the purposes for which it is being processed. This principle is particularly important in an era where vast quantities of data can be collected and stored with ease. By limiting the scope of data collection, GDPR minimizes exposure to risks associated with unnecessary or excessive data storage and use. Accuracy is another fundamental principle, emphasizing that personal data must be accurate and, where necessary, kept up to date. Inaccurate or outdated information can lead to harmful consequences for individuals, including incorrect profiling, discrimination, or denial of services. Therefore, organizations are obligated to take reasonable steps to ensure the accuracy of the data they process (Hallinan & Zuiderveen Borgesius, 2020).

The principle of storage limitation specifies that personal data should not be

retained longer than necessary to fulfill the purposes for which it was collected. Organizations must establish retention policies to ensure that data is deleted or anonymized once it is no longer needed, reducing the risk of breaches and unauthorized access. Integrity and confidentiality are essential to GDPR's framework, requiring robust security measures to protect personal data from unauthorized access, loss, or damage. This principle underscores the importance of technical and organizational safeguards, such as encryption, access controls, and regular security assessments, in maintaining the confidentiality and integrity of personal data. Finally, the accountability principle places the responsibility squarely on organizations to demonstrate compliance with GDPR requirements (Karjalainen, 2022).

This principle goes beyond mere adherence to the rules; it requires organizations to document their compliance efforts, conduct impact assessments, and maintain a proactive approach to data protection. The principle of accountability has become a defining feature of GDPR, emphasizing that compliance is an ongoing process rather than a one-time effort. In addition to these principles, GDPR grants individuals a range of rights designed to empower them and give them greater control over their personal data. Among these rights is the right to access, which allows individuals to obtain confirmation from organizations as to whether their data is being processed, as well as access to the data itself. The right to rectification enables individuals to have inaccurate or incomplete data corrected, while the right to erasure, commonly referred to as the "right to be forgotten," allows individuals to request the deletion of their personal data under specific circumstances (Lindsay, 2014).

The regulation also provides individuals with the right to data portability, which enables them to obtain and reuse their personal data across different services in a machine-readable format. Additionally, individuals have the right to object to certain types of data processing, including direct marketing and processing for scientific or historical research purposes, provided there are no overriding legitimate grounds for processing. One of the most significant procedural requirements introduced by GDPR is the obligation for organizations to notify data protection authorities of data breaches within 72 hours of becoming aware of them. This breach notification requirement enhances transparency and ensures that affected individuals are informed in a timely manner, allowing them to take appropriate measures to mitigate potential harm. GDPR also establishes stringent penalties for non-compliance, including fines of up to €20 million or 4% of an organization's annual global turnover, whichever is higher (De-Yolande, Doh-Djanhoundji, & Constant, 2023).

These severe penalties underscore the importance of compliance and serve as a strong deterrent against data protection violations. The financial and reputational consequences of non-compliance have prompted organizations to prioritize data protection and invest in compliance measures. Despite its strengths, GDPR has faced criticism and challenges, particularly concerning its extraterritorial scope. The regulation applies to organizations outside the EU that offer goods or services to individuals within the EU or monitor their behaviour. While this approach ensures

comprehensive protection for EU citizens, it has led to tensions with other jurisdictions, such as the United States, where data protection laws are more fragmented and sector-specific. For instance, the California Consumer Privacy Act (CCPA) provides limited protections compared to GDPR, creating inconsistencies in cross-border data handling practices (Hoofnagle, van der Sloot, & Zuiderveen Borgesius, 2019).

Moreover, many regions, particularly in Africa, lack robust data protection frameworks, leaving individuals vulnerable to privacy violations and exploitation. While the African Union adopted the Convention on Cyber Security and Personal Data Protection in 2014, the implementation of comprehensive data protection laws across the continent has been uneven. This disparity highlights the need for greater international cooperation and capacity-building to ensure that individual's worldwide benefit from strong data protection measures. GDPR represents a landmark in data protection legislation, setting a global standard for safeguarding personal data and addressing the challenges of the digital age. Its principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability provide a comprehensive framework for data protection (Shao et al., 2024).

IV. Discussion

The GDPR's comprehensive nature contrasts with fragmented frameworks globally. In the United States, sectoral laws create gaps in data protection, leading to inconsistencies in safeguarding personal data. For example, while GDPR mandates unified and stringent measures across the EU, U.S. frameworks such as HIPAA, COPPA, and the CCPA are limited in scope, resulting in loopholes that leave individuals vulnerable. The issue of federal oversight further complicates matters, as privacy laws vary significantly between states. Asia's diverse regulatory environment demonstrates both advancements and challenges. Nations like Japan and South Korea have developed comprehensive frameworks comparable to GDPR, but emerging economies such as India face hurdles in balancing privacy with economic priorities. India's draft legislation, for instance, includes provisions for government access to personal data, which critics argue undermines privacy rights (Kennedy, Doyle, & Lui, 2009).

China's Personal Information Protection Law (PIPL) exemplifies a state-controlled approach that integrates robust consumer protections with extensive government surveillance capabilities. Africa's struggle with enforcement further complicates the global privacy landscape. While frameworks like South Africa's POPIA show promise, enforcement mechanisms are often hindered by limited resources and infrastructure. The lack of awareness about privacy rights among citizens exacerbates the situation, making individuals more susceptible to data exploitation by corporations and state entities. Regional disparities within Africa also mean that cross-border data flow agreements remain elusive, challenging businesses

operating across multiple jurisdictions (Geller, 2020).

Another critical issue is the operational burden on multinational corporations. Companies must navigate complex and often conflicting legal requirements to ensure compliance across regions. For example, transferring data between the EU and the U.S. requires adherence to Standard Contractual Clauses (SCCs), a process criticized for being cumbersome and costly. These challenges highlight the need for global standards that prioritize interoperability and ease of compliance without compromising privacy protections. For individuals, the lack of harmonization results in a disparity of rights. Residents of the EU benefit from GDPR's extensive safeguards, while those in countries with weaker frameworks often lack recourse in cases of data breaches or misuse. This digital divide exacerbates inequalities, limiting participation in the global digital economy for vulnerable populations (Cory, Dick, & Castro, 2020).

The ethical implications of inconsistent data protection also warrant consideration. Organizations operating in regions with lax privacy laws may exploit these gaps, leading to unethical practices such as data mining, profiling, and discriminatory algorithmic decision-making. Furthermore, the reliance on data localization policies by some nations, intended to enhance sovereignty, can lead to fragmentation and hinder global data flows. To further contextualize the impact of GDPR versus weaker protections, examining specific global case studies offers insights into challenges and progress worldwide (Scheibner et al., 2020).

The United States remains a unique case due to its lack of a unified federal data protection law. Instead, sectoral legislation governs specific areas such as healthcare (HIPAA), financial data (GLBA), and children's data (COPPA). The California Consumer Privacy Act (CCPA) adds another layer of complexity, offering protections similar to GDPR but only within California. The U.S.'s emphasis on corporate interests and national security often overshadows individual privacy concerns, as evidenced by the revelations of mass surveillance programs such as PRISM. The Schrems II decision invalidating the EU-U.S. Privacy Shield further highlights the incompatibility between GDPR and U.S. surveillance practices (Hornuf, Mangold, & Yang, 2023).

Asian countries present diverse approaches to data protection. Japan's APPI aligns closely with GDPR, providing robust protections and facilitating cross-border transfers through its adequacy agreement with the EU. South Korea's PIPA is another strong framework, emphasizing stringent breach notification and accountability measures (Ko, Leitner, Kim, & Jeong, 2017). Conversely, India's proposed data protection law contains GDPR-inspired elements but introduces controversial provisions like mandatory data localization and broad government exemptions, which raise concerns over state-led surveillance Africa faces significant challenges in implementing data protection laws. While countries like South Africa (POPIA) have developed comprehensive frameworks, enforcement mechanisms remain underfunded and inconsistent across the continent.

Nigeria's Data Protection Regulation (NDPR) and Kenya's Data Protection Act

represent progress but face hurdles such as limited public awareness and technological infrastructure. The lack of harmonization within the African Union further exacerbates compliance difficulties for businesses operating across borders. Achieving global harmonization requires multilateral collaboration among governments, corporations, and civil society (Makulilo, 2016). International organizations such as the OECD and the ITU can facilitate dialogue and establish baseline privacy standards that respect regional contexts while ensuring fundamental protections. Efforts should focus on creating interoperable frameworks that prioritize transparency, accountability, and individual empowerment.

Conclusion

The disparity between the General Data Protection Regulation (GDPR) and weaker frameworks highlights the fragmented and inconsistent nature of the global regulatory landscape regarding data protection and privacy. GDPR, widely regarded as one of the most comprehensive and stringent privacy laws in existence, has established a benchmark for data protection worldwide. It enforces strict guidelines for handling personal data, requiring transparency, accountability, and user consent, while providing robust rights for individuals. However, despite its influence, many regions continue to operate under weaker or less uniform frameworks that fail to match GDPR's scope and rigor. This fragmentation creates significant challenges, both for protecting individual privacy rights and for fostering seamless international data flows. Without unified global standards, disparities in enforcement and protection levels persist, often leaving individuals in less regulated jurisdictions vulnerable to misuse or exploitation of their personal information.

Achieving global privacy standards, however, is not a straightforward process. The harmonization of data protection regulations on a global scale requires meaningful international cooperation among governments, regulatory bodies, and other stakeholders. Such collaboration is necessary to address the diverse cultural, economic, and political factors that influence each region's approach to privacy. While GDPR offers an ideal model for strong privacy protections, its direct implementation may not be feasible for all regions due to differing levels of technological infrastructure, economic priorities, or cultural norms surrounding data usage. For instance, developing nations may prioritize economic development over stringent privacy regulations, leading to weaker frameworks that prioritize business interests over individual rights. International efforts to harmonize privacy laws must, therefore, take these regional contexts into account to ensure that solutions are both practical and effective across different socio-economic environments.

Balancing regional contexts with universal protections is a delicate but critical task in the pursuit of global privacy standards. Harmonization efforts must strive to create a baseline level of data protection that transcends borders while allowing room for localized adaptations. This approach can ensure that privacy protections are universally recognized as fundamental rights, irrespective of geography or jurisdiction. Such protections are essential in an era of rapid digitalization, where data flows

seamlessly across borders and personal information becomes increasingly valuable. Treating privacy as a fundamental right underscores the need for universal safeguards that prioritize individuals' autonomy and dignity, rather than relegating such protections to a privilege accessible only to those in regions with advanced regulatory frameworks like GDPR.

The adoption of GDPR principles by some non-European countries demonstrates the potential for harmonization, but achieving comprehensive global standards requires more structured and inclusive dialogues. Multilateral agreements, international frameworks, and shared best practices could bridge the gaps between regions with varying regulatory strengths. Ultimately, the goal is to ensure that every individual, regardless of their location, benefits from robust and enforceable privacy protections. As Voigt and von dem Bussche (2017) argue, privacy should not be treated as a privilege afforded to select populations but as an inherent right that safeguards personal autonomy in the digital age. Through collaborative efforts and an emphasis on shared values, the global community can work toward a more unified and equitable approach to data protection.

Bibliography

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

AllahRakha, N. (2024). Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. *Lex Scientia Law Review, 8*(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081

Cory, N., Dick, E., & Castro, D. (2020, December 17). *The role and value of standard contractual clauses in EU-U.S. digital trade*. Information Technology and Innovation Foundation. https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/

Djanhoundji, T., & Constant, G. (2023). Breach notification in the General Data Protection Regulation. *Voice of the Publisher*, *9*, 334–347. https://doi.org/10.4236/vp.2023.94026

Geller, A. (2020). How comprehensive is Chinese data protection law? A systematisation of Chinese data protection law from a European perspective. *GRUR International*, *69*(12), 1191–1203. https://doi.org/10.1093/grurint/ikaa136

Gulyamov, S., & Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.119

Hallinan, D., & Zuiderveen Borgesius, F. (2020). Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle. *International Data Privacy Law*, *10*(1), 1–10. https://doi.org/10.1093/idpl/ipz025

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hornuf, L., Mangold, S., & Yang, Y. (2023). Data protection law in Germany, the United States, and China. In *Data privacy and crowdsourcing* (pp. 49-68). Advanced Studies in Diginomics and Digitalization. Springer. https://doi.org/10.1007/978-3-031-32064-4_3

Karjalainen, T. (2022). All talk, no action? The effect of the GDPR accountability principle on the EU data protection paradigm. *European Data Protection Law Review, 8*(1), 19–30. https://doi.org/10.21552/edpl/2022/1/6

Kennedy, G., Doyle, S., & Lui, B. (2009). Data protection in the Asia-Pacific region. *Computer Law & Security Review*, *25*(1), 59–68. https://doi.org/10.1016/j.clsr.2008.11.006

Ko, H., Leitner, J., Kim, E., & Jeong, J. (2017). Structure and enforcement of data privacy law in South Korea. *International Data Privacy Law*, *7*(2), 100–114. https://doi.org/10.1093/idpl/ipx004

Lindsay, D. (2014). The 'right to be forgotten' in European data protection law. In N. Witzleb, D. Lindsay, M. Paterson, & S. Rodrick (Eds.), *Emerging challenges in privacy law: Comparative perspectives* (pp. 290–337). Cambridge University Press.

Makulilo, A. B. (Ed.). (2016). *African data privacy laws*. Law, Governance and Technology Series. Springer Cham. https://doi.org/10.1007/978-3-319-47317-8

Mamanazarov, S. (2024). Intellectual Property Theories as Applied to Big Data. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.164

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: A global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences, 6*(1). https://doi.org/10.51594/ijarss.v6i1.733

Rizka, R. (2024). Legal Protection for Consumers Who Buy and Sell Used Goods on Facebook. *International Journal of Law and Policy*, *2*(4), 44–54. https://doi.org/10.59022/ijlp.165

Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J. R., Raisaro, J. L., Hubaux, J.-P., Fellay, J., & Vayena, E. (2020). Data protection and ethics requirements for multisite research with health data: A comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences*, *7*(1), lsaa010. https://doi.org/10.1093/jlb/lsaa010

Shahzady, R. (2024). The Role of Social-Media for Micro-Entrepreneurship of Young Startups. *International Journal of Law and Policy*, *2*(6), 10–22. https://doi.org/10.59022/ijlp.194

Shao, D., Ishengoma, F., Nikiforova, A., & Swetu, M. (2024). Comparative analysis of data protection regulations in East African countries. *Digital Policy, Regulation and Governance*, *ahead-of-print*. https://doi.org/10.1108/DPRG-06-2024-0120

Singh, D. S., & Prerna. (2024). Regulation of cross-border data flow and its privacy in the digital era. *NUJS Journal of Regulatory Studies*, *9*(2). https://doi.org/10.69953/nurs.v9i2.9

Singla, A. (2024). The evolving landscape of privacy law: Balancing digital innovation and individual rights. *Indian Journal of Law*, *2*(1), 1–6. https://doi.org/10.36676/ijl.v2.i1.01

Tarran, B. (2018). What can we learn from the Facebook—Cambridge Analytica scandal? *Significance*, *15*(3), 4–5. https://doi.org/10.1111/j.1740-9713.2018.01139.x

Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer Cham. https://doi.org/10.1007/978-3-319-57959-7

Zelianin, A. (2022). Personal data as a market commodity in the GDPR era: A systematic review of social and economic aspects. *Acta Informatica Pragensia*, *11*(1), 123–140. https://doi.org/10.18267/j.aip.168