

Towards Legal Regulations of Data Privacy in regards to Jordanian Banks Sharing Data with Third Parties

Lubiana Hanna Ammari¹, Ali Khaled Qtaishat²

Abstract

This research explores the impact of the absence of comprehensive data privacy regulations in Jordan, particularly on banks when sharing customer data with third parties. While developed countries have stringent regulations like the GDPR and CCPA, Jordan lacks such a framework. Interviews with expertise reveal varying perceptions of existing regulations and their enforcement. The study urges Jordanian lawmakers to prioritize and establish robust data privacy laws, akin to the GDPR, prioritizing user rights. Banks are advised to enhance employee competence, adhere to regulatory standards, conduct due diligence, and ensure proper oversight of third-party data sharing.

Keywords: *Data Privacy, GDPR and CCPA.*

I. Introduction

Banks are not just repositories for financial assets but also custodians of vast customer data, spanning from basic personal details to intricate information like IP addresses and location data . A crucial ruling in Digital Rights Ireland established the importance of metadata in data privacy, categorizing it as personal data due to its potential to indirectly identify individuals .

Sensitive data, including biometric and genetic information, as well as racial or ethnic origins, demands heightened protection due to the risks it poses to individuals' rights and freedoms . Banks also treasure financial and investment information, offering insights into income, wealth, and creditworthiness . In an era of digitalization and a globalized economy, digital financial services have seen a surge, accelerated by the COVID-19 pandemic.

However, this digital transformation brings privacy and security risks. Cyberattacks, data breaches, and identity theft loom large as potential threats . A supervision report by the European Central Bank highlighted cybercrime and IT deficiencies as top risks for the Eurozone banking system, especially with the increasing use of cloud services and digitalization .

Countries are racing to establish data privacy policies and regulations, but their approaches differ. Some nations, like Switzerland, maintain strict banking confidentiality, while others, like Jordan, allow data sharing under specific legal conditions. Banks are also increasingly sharing data with third-party service providers , raising concerns about cybersecurity.

¹ Master of Laws in Internet Law and Policy, Researcher, Digital Product Owner - Capital Bank, Head Office Al Abdali, Amman, Jordan, lubianaha.Ammari@capitalba.nk.jo

² Professor, Private Law Department, Faculty of Law, Al-Ahliyya Amman University, Amman-Jordan, aliqtaishat@ammanu.edu.jo

The "third-party problem" arises from the varying cybersecurity measures of these providers. Recent data breaches, like the one involving Morgan Stanley, underscore the risks associated with third-party vendors. As the financial sector becomes a prime target for hackers, a significant gap exists between developing and developed countries regarding data protection laws. Developing nations often lag in both the adoption and enforcement of these regulations .

This research focuses on this data privacy gap, with Jordan as a case study. Jordan, despite its progressive constitution and population of around 10,806 , lacks comprehensive data privacy regulation, relying on a patchwork of laws and regulations. Jordanian banks, supervised by the Central Bank of Jordan (CBJ), dominate the financial sector, with JD 54.7 billion in assets by the end of 2019 .

The study aims to understand privacy concepts, examine data privacy regulations in the EU and the US, evaluate Jordan's regulatory landscape, and analyze the consequences of lacking comprehensive data privacy regulations for Jordanian banks sharing data with third parties. Interviews with financial representatives will contribute to these objectives.

The central research question is: "What is the effect of the absence of comprehensive data privacy regulation on Jordanian banks sharing data with third parties?" This research aims to illuminate the challenges, identify potential solutions, and offer insights into this critical issue.

In conclusion, the financial sector's digitalization raises data privacy and security concerns. While countries strive to enact regulations, discrepancies exist between nations. This research delves into the data privacy gap, using Jordan as a case study, to provide valuable insights into data privacy in the digital era.

II. Methodology

The research primarily employs a qualitative approach, given its theoretical nature, heavily relying on existing data privacy regulation literature. This method emphasizes in-depth data collection and analysis to attain contextual understanding, following an inductive approach to generate theory from research and data analysis .

Both primary and secondary research methods will be used. Secondary research, or desk research, draws from published sources like books, scholarly articles, reports, and handbooks, critically examined to support rational arguments .

For primary data collection , semi-structured interviews with lawyers and data privacy professionals will be conducted . This approach, deemed effective in qualitative research, allows for prepared questions and identified themes to explore the under-researched topic. Open-format and semi-structured questions will reveal diverse perspectives.

Keyword searches, including data privacy, data sharing, cloud computing, FinTechs, financial institutions, data privacy in Jordan, Central Bank of Jordan, and open banking, were conducted on platforms like Google Scholar, Westlaw, Lexis Library, HeinOnline Law Journal Library, BAILLI, Emerald, Jstor, and Research Gate to access relevant data and literature.

III. Notion of Privacy

Privacy, a concept whose definition has evolved throughout history , is deeply influenced by economic, political, cultural, religious, and societal factors . Germany, once notorious for abusing personal data during the Nazi era, now boasts some of the world's strongest privacy regulations . Individual attitudes towards privacy vary widely, often depending on the context. While people may willingly share medical data with trusted entities, they

may vehemently oppose such sharing if it jeopardizes their financial or employment prospects.

Privacy is a debated concept

The definition of privacy has been a subject of profound philosophical debate . Privacy scholar Daniel Solove suggests that it is a multifaceted and intricate concept that defies a single, concise definition. One of the earliest legal definitions of privacy emerged in 1890 when lawyers Samuel Warren and Louis Brandeis coined the term as the "right to be let alone." This expansive definition gained popularity in US jurisprudence and laid the foundation for discussions about privacy.

Privacy concerns have evolved in tandem with technological advancements. Innovations like portable cameras and audio recordings raised issues about intrusions into private life. Scholar Alan Westin contributed to the discourse by emphasizing individuals' rights to control the disclosure and dissemination of their personal information .

More recently, Solove pointed out that existing conceptions of privacy were often either overly narrow or excessively broad . He categorized privacy into six dimensions: the right to be left alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy .

The emergence of Information Technology (IT) has further complicated the definition of privacy , giving rise to debates about its boundaries. Privacy intersects with concepts like anonymity, confidentiality, secrecy, and security ethics. Anonymity , for instance, allows individuals to protect their identity , facilitated by technologies such as "Anonymizers."

Confidentiality, especially under British law, closely relates to privacy , focusing on the externalization of specific data. Security, while essential for privacy, is a subset of it , primarily addressing data protection, integrity, authentication, and confidentiality. Data privacy and ethics are interconnected, with ethical dimensions providing guidance for data usage, adoption, and sharing.

In summary, privacy is a multifaceted concept whose definition is context-dependent and subject to ongoing philosophical and societal discussions. Its historical evolution mirrors the shifts in technology and societal norms. Privacy encompasses various facets, including the right to control personal information, the desire for secrecy, and the need for data security, all while adhering to ethical considerations. Understanding privacy necessitates recognizing its complex relationship with other constructs and acknowledging its evolving nature in an increasingly digital world.

Information Privacy

The right to personal data protection and privacy, referred to as "the right to respect for private life" in European legislation, are related but distinct rights. Privacy includes protection from interference, while personal data protection, often called "informational privacy," has led to specific legislation regulating data processing . Empirical studies explore the "informational privacy calculus," where individuals weigh data-sharing costs and benefits . This calculus considers the one-dimensional construct of information privacy risk (data loss) and the benefits, like social adjustments and financial rewards . The nature of data collected , such as behavior or location data, influences people's reactions . Privacy discussions extend to various sectors, political contexts, and technological applications.

Data Collection

Banks leverage data to enhance customer experiences, refine services, and employ Customer Relationship Management (CRM) systems for targeted marketing . Data underpins both online and offline banking operations and extends to acting as intermediaries for non-financial services like budgeting, loyalty programs, and travel

services. By adopting customer-centric data-driven approaches, banks improve lending decisions, enhance customer lifetime value, and boost Return on Investment (ROI) . Beyond basic customer information, banks now collect shopping behavior, spending analysis, and biometric data (e.g., fingerprint, facial, and voice recognition) for authentication and security . Jordan pioneered iris-enabled ATMs , increasing convenience, security, and inclusivity, while also monitoring non-identifying data for fraud prevention

Data Sharing

Banks have various reasons to share customer data with third parties. This sharing is essential for complying with legal requirements, such as court orders and the Foreign Account Tax Compliance Act (FATCA), which mandates reporting on US account holders and foreign assets . Failing to do so can result in hefty fines. Banks also share data to report suspicious customer activity to combat money laundering and terrorist financing, as exemplified by Australia's Westpac bank. Additionally, they provide customer information to credit bureaus for consumer reports and to third-party service providers for affinity reward programs and marketing various products. The rise of FinTechs, leveraging digital technologies, is expected to further fuel data sharing. To efficiently manage the vast amount of data collected , banks also collaborate with cloud service providers . Moreover, the European Union's Payment Services Directive (PSD2) has pushed banks to offer open APIs, promoting competition and innovation in financial services while improving financial inclusion and access.

IV. Overview of Privacy Legislation Development

In today's interconnected and digitized banking landscape, data privacy is of paramount importance. With the outsourcing of back-office functions and the adoption of Open Banking, safeguarding data privacy becomes crucial. This chapter examines the development of privacy legislation in Europe, the United States, and Jordan.

Overview of Privacy Legislation Development in Europe

Europe has a long history of valuing privacy, stemming from the need to protect against the extensive surveillance during the Nazi regime. After World War II, data protection gained prominence, leading to comprehensive data protection legislation. In 1970, Germany's Hesse state passed the first data protection law, followed by Sweden. However, these early laws had limitations, such as the need for export licenses to transfer data abroad. European countries like Denmark, France, and Austria also enacted data protection laws before international frameworks were established.

The right to data protection is recognized as a fundamental right in the Treaty on the Functioning of the EU (TFEU) and the Charter of Fundamental Rights of the European Union (CFHR). Convention 108, adopted in 1980, played a vital role in data protection, although it had limitations regarding data transfer. Forty years later, Modernized Convention 108 remains a crucial international instrument for data protection.

Directive 95/46/EC (DPD), enacted in 1995, was the primary data protection law in the EU until 2018. While it influenced data processing practices and created supervisory authorities, it had limitations due to varying transpositions by Member States. The General Data Protection Regulation (GDPR), implemented in 2018, aimed to harmonize national privacy laws and address new data challenges. It expanded its geographic reach and focused on individual control over personal data, enforcement mechanisms, and substantial fines for non-compliance.

Overview of Privacy Legislation Development in the US

Privacy laws in the US are sector-specific, with statutes scattered across criminal law, common law torts, and state laws. Early legislation emerged in response to technological advancements, such as California's ban on wiretapping in 1862. The Privacy Act of 1974 addressed federal government record-keeping, but it had limitations like the "routine use" exception.

Several statutes aimed to protect financial privacy, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act. However, privacy laws were often criticized for their complexity and limited protections.

With the rise of the internet, the Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 to address data sharing and protection by financial institutions. Despite introducing opt-out provisions, the law faced criticism for complexity and low opt-out rates.

States like California responded by passing the California Consumer Privacy Act (CCPA) in 2018. This comprehensive law provided consumers more control over their data, transparency requirements for organizations, and regulatory fines for non-compliance.

Overview of Privacy Legislation Development in Jordan

Privacy is a constitutional right in Jordan, with constitutional provisions protecting private life, personal freedom, inviolability of houses, and secrecy of communications. These constitutional protections are superior to other legislation in Jordan.

Jordan has ratified various international and regional instruments related to privacy, including the Cairo Declaration on Human Rights in Islam and the Arab Charter on Human Rights. On the international level, Jordan is a signatory to the Universal Declaration of Human Rights (UDHR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), and the International Covenant on Civil and Political Rights (ICCPR).

Despite these protections, infringements on privacy rights in Jordan have been reported, as highlighted in Jordan's Human Rights report for 2018.

In conclusion, data privacy legislation has evolved significantly in Europe, the US, and Jordan. The GDPR represents a landmark in European data protection, while the US has seen sector-specific laws and state-level initiatives like the CCPA. Jordan places importance on constitutional protections and international agreements but faces challenges in practice.

Data Protection and Privacy Draft Law

Jordan lacks comprehensive data protection legislation, but efforts have been made to introduce a strict law, the Personal Data Protection Law Draft, since 2014. The law aims to protect individuals' data privacy amid technological advancements and align with international agreements, especially those involving the European Union. Public consultations and revisions of the draft have taken place, involving various governmental bodies and organizations. However, concerns remain, including the proposed structure of the Data Protection Commission, suggesting a conflict of interest, and vague provisions allowing data processing for "security purposes" or the "public interest" without explicit consent. The draft awaits approval procedures before becoming law.

Jordanian Penal Code No. 16 of 1960

Jordan's penal code enacted in 1960 includes limited provisions that safeguard the right to privacy. Virtue to Article 384, any peaking, eavesdropping, audio recording or any other mean that breaches the private lives of others, is a crime punished with a maximum of three months' imprisonment, which can further be multiplied if repeated.

Jordanian Civil Code No. 43 of 1976

The Civil code was enacted in 1976. It replaced Majallah al-Ahkām al-adliyyah of 1876. The latter represents the Civil Code of the Ottoman Empire, which was applied by most Arab countries that were ruled by the Ottomans. Nevertheless, Majallah al-Ahkām al-adliyyah, which is highly influenced by Islamic Law, is still applied by Jordanian courts as long as its rules do not contradict the Jordanian Civil Code provisions.

Article 48 of the Jordanian Civil Code provides for a range of rights inherent to human status. Consequently, as the right to privacy is considered one of the rights inherited in the personality of a human, it falls under the protection of Article 48. Moreover, this recognition entails anyone subjected to unlawful infringement on any rights inherent in his personality to request this infringement be stopped along with compensation for the damages he may have suffered. Nevertheless, the mere assault in itself enables the cessation of this assault without the need to prove any harm.

Notwithstanding, principles under the Jordanian Civil Code are considered general provisions that any court of law can rely on in the absence of legislation related to the matter in question; accordingly, relevant case law decisions refer to it as “the father of all laws”.

The Telecommunications Law No. 13 of 1995

The telecommunications sector witnesses rapid and robust change in new technologies and policies worldwide; likewise, the Jordanian telecommunications sector has undergone remarkable transpositions. Jordan was the first Arab country to liberalize its telecommunications sector completely. The first step towards liberalization was enacting the Telecommunications Law No 13 of 1995. This act ended a monopoly stage in provided services by incorporating provisions designed to foster a fair and competitive regulatory setup. Thus, the sector witnessed an evident decrease in service prices as well as a growing number of internet service providers (ISPs) and communication product suppliers.

From a different perspective, under the Telecommunications Law, service providers are restricted from sharing their customers' calls and communication content with third parties or conducting customer telephone tracking as stipulated in Articles 56,71, and 77. However, Article 29 (g) sets forth exceptions to disclosing customer calls and communications; upon judicial or administrative orders.

Banking Law of 2000

Virtue to Article 72 of the Banking Law of 2000 and its updated amendments, the bank is committed to safeguarding the confidentiality of bank clients' information, and this confidentiality is to be maintained after the bank-client relationship is ended for any reason. Furthermore, this latter provision, along with Article 74 and 93, defines that client data is permissible to be disclosed against a set of rules such as the presence of the customer's written consent or a decision of judicial authority.

Nevertheless, following Article 32 of the Banking Law, all banks must establish an audit committee consisting of a chairperson and at least two members that should be non-executive directors to promote their independence. The audit committee, among other duties, is responsible for ensuring the accuracy and integrity of procedures and compliance with laws and regulations.

Anti-Money Laundering and Counter-Terrorist Financing Law for the year 2007

While remittances play a vital role in the Jordanian economy and significantly promotes its monetary and fiscal policies, they can be a mean used for money laundry and terrorist financing. The most exposed sectors to money laundry risks are the banking and money

exchange sectors as 98.4% of the Suspicious Activity Reports (SAR), are received from banks and exchange companies.

Jordan adopted its first regulation concerning the Anti-Money Laundering Law in 2007. While Article 13 of the Anti-Money Laundering Law lists all parties and entities obliged to comply with the provisions stipulated in this act, Article 16, on the other hand, exempts these mentioned parties from any liability, whether penal, civil or administrative, along with disciplinary liabilities, when disclosing suspected customer data.

This latter law was further amended in 2015 to widen its scope and criminalize terrorist financing. The amended provisions reinforced the Anti-Money Laundering Unit's (AMLU) independence and granted more power for judges and public prosecutors to track funds, confiscate it and impose sanctions.

Notwithstanding, the Middle East and North Africa Financial Action Task Force for combating Money Laundering and Terrorist Financing (MENAFATF) issued several recommendations in response to its 2018 evaluation of Jordan's compliance status with the FATF 40 Recommendations in addition to the extent of system measures effectiveness of the anti-money laundering and counter-terrorist financing. It requested Jordan's law enforcements agencies and judicial authorities to share information with the AMLU in a safer manner that mitigates any potential breaches of confidentiality.

Credit Information Law No. 15/2010

The last quarter of 2016 witnessed the launching of the first credit bureau company (CRIF) services in Jordan. It assists banks and credit providers in making credit decisions based on an accurate assessment of customers' ability to pay and thus pricing financial products and services. CRIF was established after enacting the Credit Information Law of 2010 and the Credit Information Companies System of 2011.

According to Article 8 (a and b), disclosure of customers' information is prohibited without a written consent to share credit status with banks and credit providers. However, the third point of the same article stipulates that the customers' credit status can be revealed to the banks and credit providers requesting information without the customer's approval, subject to obtaining the Central Banks Governor's approval. The Credit Information Act furtherly offered the customers a range of considerable rights in line with counterparty laws. These rights are evident in Article 9, which gives the customer the right to be informed of the purpose of obtaining his credit information, view, and request its correction.

From a different perspective, the Credit Information Law was issued as an interim law. At the time of issuing the act, the Minister of State for Media Affairs and Communication, the official spokesman for the Government, stated the objectives and benefits of enacting the Credit Information Law. He expressed that such a law regulating credit information would boost the Kingdom's ranking in the international credit information index. However, he further asserted that any delay in issuing the legislation regulating credit information could be a catalyst for the continuation and compound of the financial and economic crisis for an extended period.

Notwithstanding, the Jordanian constitutional amendments, which took place in 2011, determined the cases in which temporary laws can be issued, such as emergencies and disasters. However, interim laws need to be presented before the Parliament in its first session. Hence, if the period lapses and the interim law is not decided upon, it must be declared invalid immediately. On the other hand, the Higher Council for the Interpretation of the Constitution addressed this issue in its interpretative decision in 2012 and excluded all temporary laws referred to the House of Representatives before the constitutional amendments came into force in 2011 from the specified period. That being said, the Credit Information Law has remained standing as an interim law for over a decade.

Cybercrime Act No 27 of 2015 (Cybercrime draft law)

The Information System Crimes Law No (30) of 2010 was the first Jordanian law on cybercrimes. It included computer-enabled crimes in addition to offences committed by the use of electronic devices. It was adopted as a response to the lacunae in the former law; the Electronic Transactions Act No (85), 2001, which by its end had only focused on e-commerce and lacked any provisions related to computer-related offenses. The Jordanian Government then made a fast move by adopting an interim law. However, with the absence of parliamentary review, the Information System Crimes Law of 2010 witnessed substantive criticism. Though it incorporated major cyber-crimes, it failed to include all known computer-related crimes in line with legislation of other countries. In the same context, not all provisions related to privacy protection were included and were characterized as being vague. In another vein, the Law was found to impose more restrictions on freedom of expression, which was the primary concern of the Human Rights Watch, which acknowledged the act to be inequitable for the foreseen reasons. As a result, the Cybercrime Law was adopted in 2015, updating and replacing the Information System Crimes Law.

The updated Cybercrime law defines a set of penalties for activities related to privacy and data protection. Virtue to Article 3, anyone who deliberately accesses an information system or a website without permission will be fined, and the same applies to copying or intercepting users' data from a website. Moreover, unlawfully modifying, deleting, or interfering with a computer system or platform is also criminalized under this latter act, along with fraudulent use or alteration of data and systems. Nevertheless, article 6 of the Cybercrime Law sets forth penalties for falsely acquiring financial data, including credit cards or data used to execute electronic financial or banking transactions.

However, in December 2018, the Jordanian Government anticipated a range of amendments to the Cybercrime Law. These amendments were encountered with massive criticism as they were perceived to violate individuals' right to privacy and restrict their freedom of expression online. For instance, the proposed amendment to Article 2 entailed smartphone apps being subject to mass surveillance. Besides, other provisions were feared to be taken into an advantage to target activists and human rights defenders. These uncertainties were rationalized with the vague language used in the content of the proposed provisions, which could be interpreted in a blurred manner that streaks the line between hate speech and legitimate criticism of public figures on social media.

In the same context, following the Human Rights Council's Universal Periodic Review (UPR) session held in November 2018, Jordan was addressed with recommendations related to concerns of data privacy. The UPR requested Jordan to amend its cybercrime law to counterpart the International Covenant on Civil and Political Rights. Nevertheless, the debated Cybercrime law amended draft yet still stands as a draft.

The Jordanian Electronic Transactions Act of 2015

The new law sets forth the definition of the electronic signature, which is in line with the UNCITRAL Model Law on Electronic signatures of 2001. The law also explicates the three states of signature; ordinary, protected and authenticated, clarifying the characteristics of each type. In a practical approach, the Electronic Transactions Act afforded electronic records the same legal value as written documents. Likewise, it considered the electronic records associated with a protected or an authenticated signature and documents holding a traditional signature, as both to constitute the consent of the signatory, which represents the latter's approval to the signed document and both to reveal the identity of its owner. However, granting this unified level of value is subject to maintaining specific security and technical requirements for electronic records.

Though the law comprises a relatively robust legal framework, it lacks practical implementation as no licenses have been issued for any independent providers of authenticated services.

Jordan's Cybersecurity Law of 2019

Jordan recently adopted the Cybersecurity Law in 2019, which enhances the existing policy framework. It echoed the National Cybersecurity Strategy 2018-2023, which elaborated on the objectives of the strategy outlined in 2012 by the National Cybersecurity Program

(NCP). The enacted Cybersecurity Law incorporates substantive penal rules, procedural rules, and provisions related to international cooperation. Due to the importance of interagency collaboration in developing and applying cybersecurity policy, Article 3 of the Cybersecurity law urges to assemble a National Cybersecurity Council, which should include representatives from the Ministry of Digital Economy and Entrepreneurship (MoDEE), Public Security Directorate, Jordanian Armed Forces, the National Center for Security General Intelligence Department, and Crisis Management and Central Bank of Jordan. Furthermore, Article 5 of the Cybersecurity law calls for establishing a National Center for Cybersecurity responsible for cybersecurity policymaking and architecture.

Central Bank of Jordan Releases

In addition to the above laws, the central bank of Jordan enacted numerous regulations, directions, instructions, and circulars in its mission to oversight and regulate the financial sector. Primarily, the central bank of Jordan issued the Amended Corporate Governance Regulations for Banks No. 63 of 2016 and Governance and Information Management and Associated Technology Regulations No. (65) of 2016. Among other issues, aside from the enterprise and information and technology goals and the evaluation, direction, and monitoring processes, these provisions included the internal and external audit committees' structure. Moreover, it defined the latter's roles and responsibilities when performing their oversight upon data privacy and the competencies and certifications that employees need to maintain.

The CBJ further issued the Electronic Payment and Money Transfer regulations in accordance with Articles 21 and 22 of the Electronic Transactions Law No. 15 of 2015. Article 5 states the conditions and requirements for the payment services companies, including banks, as well as the minimum requirements that must be met in the operating systems and computer equipment to be efficient and safeguard data privacy when stored and transmitted. In the same context, the CBJ issued the Financial Consumer Protection Regulations for Payment and Electronic Money Transfer Companies No. (3) of 2021. This very recent regulation included provisions that protect data privacy and incorporates its principles of lawfulness, fairness, transparency, purpose limitations, accuracy, storage limitations, integrity, confidentiality, and accountability.

Besides, in 2018 the CBJ issued regulations that incorporate provisions for the adaptation to cyber risks, which regulates assigning part of the bank's operations to a third party to evaluate the associated risks and mitigation plans.

In addition, Cloud computing is a new era that avails various services over the internet that increases speed and security, and enhances productivity and scalability. Nevertheless, due to their cross transcends territorial borders, cloud computing raises legal challenges. Notwithstanding, since Jordan still has not adopted any legislation on that behalf, the Central bank of Jordan in 2018 issued a Cloud computing guideline. This guideline doesn't have any binding nature; instead, it forms a group of instructions to guide banks and financial institutions when approaching cloud service providers and enter into an agreement with them.

V. Interview Analyses and Discussion

The chapter focuses on analyzing key themes related to data privacy in Jordan through semi-structured interviews with professionals from various banks. Five main themes were explored: the adequacy of existing legal frameworks, privacy due diligence in agreements with third parties, law enforcement, data breaches, and the impact of the absence of comprehensive data protection legislation.

First, participants noted that Jordan lacks precise regulations regarding data sharing with third parties, including cloud service providers and FinTechs. They rely on general laws, banking regulations, internal policies, and best practices. Some mentioned that the Central Bank of Jordan (CBJ) has issued nonbinding guidelines for such cases.

Concerns arose regarding the absence of an independent data protection authority in Jordan. While some believed that existing regulatory bodies like the CBJ and the judiciary manage data protection, others argued that an independent authority with enforcement powers is needed to ensure compliance and build confidence.

Regarding privacy due diligence, participants were divided. Some affirmed that thorough evaluations are conducted when engaging with third parties, considering legal aspects, vendor profiles, and performance. Others disagreed, suggesting that due diligence is often insufficient.

Participants also discussed law enforcement. Many felt that data protection laws, when they exist, suffer from weak implementation and enforcement. They cited the need for clearer regulations and guidance.

Regarding data breaches, opinions varied. Some banks had documented breach policies, while others lacked clear mechanisms for reporting breaches. One manager mentioned that the CBJ enforces data breach reporting, with penalties for non-compliance.

The absence of comprehensive data protection legislation in Jordan was a significant concern. Interviewees noted potential risks, including dealing with weak third parties, data loss, unauthorized access, and reputational damage. They highlighted the impact on business expansion, particularly in targeting European and American customers. While most participants advocated for a comprehensive data protection law, some raised concerns about its complexity and potential conflicts with existing laws.

In summary, the interviews revealed a complex landscape of data privacy in Jordan. While some measures are in place, the absence of comprehensive legislation and independent oversight poses challenges for data protection, enforcement, and the growth of the banking sector in an increasingly digital world.

VI. Conclusion and Recommendations

Conclusion

The development of data privacy laws in Jordan has been slow, resulting in the absence of a comprehensive data privacy regulation akin to the EU's GDPR. Jordanian banks must rely heavily on contractual agreements with third parties, particularly when dealing with non-financial entities beyond the purview of the Central Bank of Jordan (CBJ). These contracts often contain arbitrary clauses imposed by service providers, potentially compromising data privacy and the flow of data, services, and applications.

Interview responses reveal disparities among banks in their oversight of third parties, with some mechanisms deemed inadequate in managing third-party risks. Third-party companies may engage with smaller suppliers and networks with inadequate cybersecurity and data privacy protection, posing significant risks. Banks are responsible for overseeing the security measures of third parties, but there is a lack of incentive for

third parties to enhance their cybersecurity as enforcement actions typically target banks even when breaches result from third-party shortcomings. In 2017, 56% of companies globally experienced third-party breaches, a figure likely to rise due to increased reliance on such services .

Recommendations

To address these challenges, it is crucial for Jordanian lawmakers to prioritize and expedite the adoption of a robust data privacy legal framework that places user rights above economic interests . Privacy-by-Design should be implemented to integrate privacy into data systems and technologies by default. Banks should conduct risk-based third-party due diligence and compliance checks, adhering to industry standards and frameworks like ISO 27001, Cobit 2019, PCI, and NIST.

Appointing a data protection officer (DPO) with expertise in business and technology is advisable. The DPO can facilitate compliance in third-party agreements involving personal data sharing. Additionally, there is a need to enhance the skills and qualifications of employees in data privacy-related roles through education and training.

Establishing an independent data privacy authority (DPA) is crucial to bridge the enforcement gap identified by 60% of interviewees. The DPA should have adequate funding and enforcement powers to operate independently, ensuring effective enforcement, monitoring, and redress within the banking sector.

Finally, this research explores privacy concepts, emphasizing its crucial role in human relationships and individual integrity. It highlights the rising threat to information privacy due to evolving technology. Investigating data practices, it reveals that Jordan lacks comprehensive data protection laws, relying on limited sectoral regulations. Interviews with various stakeholder's underscore concerns over data privacy gaps and challenges. Recommendations include substantial investments in secure systems, hiring data privacy experts, and due diligence when sharing customer data with third parties . Urgent enactment of data privacy laws in Jordan is advised to prevent customer trust erosion, reputational damage, and legal consequences in an increasingly global and data-driven landscape.

*Limitations of the Research Findings and Further Research

This research had limitations due to sparse literature on Jordan's data privacy and relied on qualitative interviews. Further research is needed on third-party data privacy oversight in the evolving financial services landscape.

References

Books

- Bryman A, and Bell E, *Business Research Methods* (3rd edn, Oxford University Press Inc. 2011)
- Frick T, *The Financial Technology Law Review* (2nd edn, Law Business Research Ltd 2019)
- Hair J and others, *Essentials of Business Research Methods* (2nd edn, Routledge 2015)
- Solove D, 'A Brief History of Information Privacy Law', *PROSKAUER ON PRIVACY* (PLI 2006) <<https://ssrn.com/abstract=914271>> accessed 19 July 2021
- Waldo J, Lin H, and Millett L, *Engaging Privacy and Information Technology in A Digital Age* (National Academies Press 2007)

Hand Books

- 'Handbook On European Data Protection Law' (Fra.europa.eu, 2018) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf> accessed 23 July 2021

Articles

- Abu Olaim A, and Rahman A, 'Recent Development of Anti-Money Laundering Law in Jordan' (2016) 19 *Journal of Money Laundering Control*
- Abu Sarhan A, [The principle of banking secrecy in the Jordanian banking law and Islamic law, a comparative study] (2018) 15 *The Jordanian Journal of Islamic Studies*
- Abu Trabi , [Legal Regulation of Cloud Computing Contracts Under Jordanian Law]' (2015) 17 *The Jordanian Journal of Applied Sciences (JJOAS)*
- Ackerman M, 'Privacy In Pervasive Environments: Next Generation Labeling Protocols' (2004) 8 *Personal and Ubiquitous Computing* 430
- Alkhasawneh A, 'The Future of Biometric Data Protection in Jordan in Light of the GDPR: do we Need to Comply with the GDPR?' (2020) 23 (2) *Journal of Legal, Ethical and Regulatory Issues*
- Almaharmeh M, 'Authenticity of Electronic Signature under Jordanian Legislation' (2016) 56 *JL Pol'y & Globalization* 24
- Almatarneh A, 'Telecommunications Trade Liberalisation and Individual Privacy in Jordan: Some Perspectives and Evolving Concerns' (2014) 14 *GJMBR* <<https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:38337/DS01>> accessed 31 July 2021
- Baicu C, 'The impact of financial innovation on banking regulation. Evidence from the global financial crisis' (2011) 2 *Annals of Spiru Haret University, Economic Series* 31
- Besen S, 'Competition, Privacy, and Big Data' (2020) 28 *Catholic University Journal of Law and Technology*
- Boardman R, Mullock J, and Mole A, 'Guide to the General Data Protection Regulation' [2020] Bird and Bird <[chrome-extension://oemmnrcbldboiebfnladdacbfmadadm/https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en](https://www.twobirds.com/~media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en)> accessed 18 July 2021
- Breidbach C, Keating B, and Lim C, 'Fintech: Research Directions to Explore the Digital Transformation of Financial Service Systems' (2019) 30 *Journal of Service Theory and Practice*
- Brodsky L, Oakes L, 'Data sharing and open banking' (2017) *McKinsey on Payments*
- Camp L, 'Web Security and Privacy: An American Perspective' (1999) 15 *The Information Society*
- Carr B, Pujazon D, Urbiola P, 'Reciprocity in Customer Data Sharing Frameworks' (Institute of international finance, July 2018) <https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf> accessed 24 August 2021.
- Citron D, and Henry L, 'Visionary Pragmatism and The Value of Privacy in The Twenty-First Century' (2010) 108 (6) *Michigan Law Review*
- Dinev T, and Hart P, 'Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended E-Services Use' (2006) 4 *e-Service Journal* 25
- Faqir R, 'Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) Of 2010' (2013) 7 *International Journal of Cyber Criminology* 81
- Finck M, and Pallas F, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data Under The GDPR' (2020) 10 *International Data Privacy Law*
- Freude A, and Freude T, 'Echoes of History: Understanding German Data Protection' Bertelsmann Foundation Newpolitik 2016<<https://perma.cc/GV6D-XAKL>> accessed 18 July 2021.
- Gimpel H, Rau D, and Röglinger M, 'Understanding Fintech Start-Ups – A Taxonomy of Consumer-Oriented Service Offerings' (2017) 28 *Electronic Markets*

- Giurgiu A and Lallemand T, 'The General Data Protection Regulation: A New Opportunity and Challenge for the Banking Sector' (2017) 1 *Ace Magazine et Archives Online: Fiscalité, Comptabilité, Audit, Droit des Affaires au Luxembourg* 3
- Gozman D, Hedman J, and Olsen K, 'OPEN BANKING: EMERGENT ROLES, RISKS & OPPORTUNITIES', (2018) 183 *Research Papers*
- Gozman D, and Willcocks L, 'The Emerging Cloud Dilemma: Balancing Innovation with Cross-Border Privacy and Outsourcing Regulations' (2019) 97 *Journal of Business Research*
- Greenawalt K, 'Privacy and Its Legal Protections' (1974) 2 *The Hastings Center Studies*
- Haibach G, 'Cloud Computing and European Union Private International Law' (2015) 11 *Journal of Private International Law*
- Hayajneh Z, 'Legal Surgery: The Need to Review Jordanian Civil Law' (2012) 6 *British Journal of Humanities and Social Sciences* 45
- Hourani H, and Abdallah M, 'Cloud Computing: Legal and Security Issues' [2018] 2018 8th International Conference on Computer Science and Information Technology (CSIT)
- Janger E, and Schwartz P, 'The Gramm-Leach-Bliley Act, Information Privacy, And The Limits Of Default Rules' [2002] *SSRN Electronic Journal* Kokkinis A, and Miglionico A, 'Open Banking And Libra: A New Frontier Of Financial Inclusion For Payment Systems?' (2020) 2020 *Sing J Legal Stud* 601
- Karim S and others, 'Is Big Data Too Big for SMEs in Jordan?' [2017] 2017 eighth International Conference on Information Technology (ICIT)
- Kim N, 'THREE'S A CROWD: TOWARDS CONTEXTUAL INTEGRITY IN THIRD-PARTY DATA SHARING' (2014) 28 *Harvard Journal of Law & Technology* 325
- Koops B and others, 'Typology of Privacy' (2016) 38 *University of Pennsylvania Journal of International Law* 483
- Lukács A, 'What Is Privacy? The History and Definition of Privacy' (Publicatio.bibl.u-szeged.hu, 2016) <<http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>> accessed 21 July 2021
- Maaitah T and others, 'Factors Affecting Customer's Initial Trust in Electronic Banking Services in Jordan' (2021) 7 *Multicultural Education & Technology Journal* 268
- Mattoo A, and Meltzer J, 'International Data Flows and Privacy: The Conflict and Its Resolution' (2018) 21 *Journal of International Economic Law*
- McGinity M, 'Surfing Your Turf: For a Medium that Holds Anonymity in High Regard, Privacy Is Fast Eroding' (2000) 43 *Communications of the ACM* 19
- Merlin Stone and Kevin Condron, 'Sharing Customer Data in the Value Chain' (2002) nine *Journal of Database Marketing & Customer Strategy Management*.
- Niket Nishant, 'Morgan Stanley Faces Data Breach, Corporate Client Info Stolen in Vendor Hack' (REUTERS, 8 July 2021) <<https://www.reuters.com/business/finance/morgan-stanley-says-some-personal-data-stolen-after-data-breach-2021-07-08/>> accessed 27 August 2021
- Nyemba Chisomo, 'Right to Data Privacy in the Digital Era Critical Assessment of Malawi's Data Privacy Protection Regime' (2019) *HRDA*
- Palmieri III N, 'Data Protection in an Increasingly Globalized World' (2019) 94 *Indiana Law Journal* <<https://www.repository.law.indiana.edu/ilj/vol94/iss1/7>> accessed 24 July 2021.
- Parsons M, Liu T, Willis G, 'Hong Kong's open era begins: your Open API Survival Guide' (2018) Hogan Lovells Publications >hoganlovells.com/en/publications/hong-kongs-open-era-begins-your-open-api-survival-guide> accessed 20 June 2021
- Phillip Shaverdian, 'Start with Trust: Utilizing Blockchain to Resolve the Third-Party Data Breach Problem' (2019) 66 *UCLA L Rev* 1242
- Qu S, and Dumay J, 'The Qualitative Research Interview' (2011) 8 *Qualitative Research in Accounting & Management*

- Richards N, and Solove D, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 California Law Review 1887
- Rustad M, and Koenig T, 'TOWARDS A GLOBAL DATA PRIVACY STANDARD' (2019)71 Fla L Rev 365
- Salih AL, 'Combating the Crime of Money Laundering in Light of Banking Secrecy Acts and Their Impact on Legal Liability, a Comparative Study' (2019) 91 JLPol'y & Globalization 17
- Sarathchandra D, 'Privacy Regulations in the Context of Finance: Comparison between Developing and Developed Countries' (the Repository at St. Cloud State, 2018) <https://repository.stcloudstate.edu/msia_etds/68> accessed 21 July 2021
- Schmidt J, Drews P, and Schirmer I, 'Charting the Emerging Financial Services Ecosystem of Fintechs and Banks: Six Types of Data-Driven Business Models in the Fintech Sector' [2018] Proceedings of the 51st Hawaii International Conference on System Sciences
- Shaverdian P, 'Start with Trust: Utilizing Block Chain to Resolve the Third-Party Data Breach Problem' (2019) 66 UCLA Law Review 1242
- Solove D, 'Conceptualizing Privacy' (2002) 90 Cal. L. Rev. 1087
- Solove D, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477
- Solove D, 'Understanding Privacy' [2008] Harvard University Press, Cambridge Massachusetts
- Stephen T. Margulis, 'On the Status and Contribution of Westin's and Altman's Theories of Privacy' (2003) 59 Journal of Social Issues 411
- Stone, E. F., and Stone, D. L., 'Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms' (1990) 8 Research in Personnel and Human Resources Management 349
- Susanto H, Almunawar M, Tuan Y, 'Information Security Management System Standards: A Comparative Study of the Big Five' (2011) 11 International Journal of Electrical & Computer Sciences 23
- Van der Cruijssen C, 'Payments Data: Do Consumers Want Banks to Keep them in a Safe or Turn Them into Gold?' (2019) 52 Applied Economics 609
- Warren S, and Brandeis L, 'The Right to Privacy' (1890) 4 Harvard Law Review <<https://doi.org/10.2307/1321160>> accessed 5 July 2021
- Xu H and others, 'The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services' (2009) 26 Journal of Management Information Systems 137
- Zwick D, and Dholakia N, 'Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing' (2004) 24 Journal of Macromarketing
- [Constitutional Protection of Information Privacy] (2017) Dar AlMandumah
- [Constitutional and Legal Protection of the Right to Personal Life]' (2020) 47 Dar AlMandumah

Newspaper Articles

Fox M, 'Alan F. Westin, Who Transformed Privacy Debate before the Web Era, Dies at 83' Nytimes.com (2013) <<https://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html>> accessed 20 July 2021

Ghabbon Hadeel, Legal shortcomings in protecting personal data exacerbate private ways of life [Legislative deficiencies in the protection of personal data exacerbate patterns of infringement of private life] Al Ghad (Jordan, April 07) < shorturl.at/uzPSU> accessed 25 July 2021

Powles J, 'The G.D.P.R., Europe's New Privacy Law, And the Future of The Global Data Economy' The New Yorker (2018) <<https://www.newyorker.com/tech/annals-of-technology/the-gdpr-europes-new-privacy-law-and-the-future-of-the-global-data-economy>> accessed 25 July 2021

Reports

- 'Anti-Money Laundering and Counter-Terrorist Financing Measures the Hashemite Kingdom of Jordan Mutual Evaluation Report' (MENAFATF 2019) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/MENAFATF-Mutual-Evaluation-Report-Jordan-2019.pdf> accessed 2 August 2021
- Chander A, 'Achieving Privacy Costs of Compliance and Enforcement of Data Protection Regulation' (2021) <http://hdl.handle.net/10986/35306> accessed 27 August 2021
- 'Consumer Privacy: Better Disclosures Needed On Information Sharing by Banks and Credit Unions' (United States Government Accountability Office 2020) <https://www.gao.gov/products/gao-21-36> accessed 6 August 2021
- 'Co-Submission to The Universal Periodic Review 31st Session - Jordan on the Right to Privacy' (Jordan Open Source Association, 2018) <https://jordanopensource.org/publications/1/cosubmission-to-the-universal-periodic-review-31st-session-jordan-on-the-right-to-privacy> accessed 4 August 2021
- 'Data Privacy Frameworks in MENA Emerging Approaches and Common Principles' (2019) <https://www.gsma.com/mena/wp-content/uploads/2019/06/GSMA-Data-Privacy-in-MENA-Full-Report.pdf> accessed 15 August 2021
- 'Exposed And Exploited: Data Protection in the Middle East and North Africa' (Access Now 2021) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://www.accessnow.org/cms/assets/uploads/2021/01/Access-Now-MENA-data-protection-report.pdf> accessed 10 July 2021
- European Central Bank, 'ECB Annual Report on supervisory activities' (2021) <http://tps://www.bankingsupervision.europa.eu/press/publications/annual-report/html/ssm.ar2020~1a59f5757c.en.html#toc9Banking Supervision> accessed 18 September 2021
- IFC Report' (2015) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://www.bis.org/ifc/events/7ifc-tf-report-datasharing.pdf> accessed 10 August 2021
- JORDAN BETTER WORKPLACE ASSOCIATION, 'Human Rights in Jordan: A Development and Legislative Overview' (JBWA, 2017)> http://jordanbetterworkplace.org/wp-content/uploads/2018/02/HR4U_-Human-Rights-in-Jordan_-development-and-legislative-overview-_May-2017.pdf< accessed 4 August 2021
- 'Regulatory Framework of the Oversight and Supervision Policy On the National Payments System' (Central Bank of Jordan 2018) <https://www.jopacc.com/ebv4.0/root_storage/en/eb_list_page/regulatory_framework_of_the_oversight_and_supervision_policy_on_the_national_payments_system_(2018).pdf> accessed 18 September 2021
- Robinson N, 'Review of the European Data Protection Directive' (RAND Corporation 2009) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://ico.org.uk/media/1042349/review-of-eu-dp-directive.pdf> accessed 25 July 2021
- The World Bank Group, 'DATA PRACTICES IN MENA Case Study: Opportunities And Challenges In Jordan' (World Bank Publications 2021) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://openknowledge.worldbank.org/bitstream/handle/10986/35313/Data-Practices-in-MENA-Case-Study-Opportunities-and-Challenges-in-Jordan-Findings-of-a-Data-Ecosystem-Assessment.pdf?sequence=1&isAllowed=y> accessed 20 June 2021
- 'The 2018 Financial Stability Report' (Central Bank of Jordan 2019) <chrome-extension://oemmnndcbldboiebfnladdacbfmadadm/https://www.cbj.gov.jo/EchoBusv3.0/SystemAssets/PDFs/EN/JFSR2018E%20-20-10-2019.pdf> accessed 4 July 2021
- 'Universal Periodic Review - Jordan' (October 2018). Ohchr<https://www.ohchr.org/EN/HRBodies/UPR/Pages/JOindex.aspx> accessed 30 July 2021

Blogs

- Adam Deakin, 'GDPR Timeline: A History of Data Protection' (Vuture July 2017) <<https://vutu.re/resources/blog/gdpr-timeline--a-history-of-data-protection.aspx>> accessed 18 September 2021
- DIVIJ JOSHI, 'Privacy Theory 101: Warren And Brandeis'S 'The Right To Privacy' – Law, Affect And The 'Right To Be Let Alone' - Centre For Law & Policy Research' (Centre for Law & Policy Research SEPTEMBER 25, 2020) <<https://clpr.org.in/blog/privacy-theory-101-warren-and-brandeis-law-affect-and-the-right-to-be-let-alone/>> accessed 20 July 2021
- Duryea A, 'Lesson #3 From A Data Scientist: The Difference Between First-Party and Third-Party Data' <<https://www.lytics.com/blog/lesson-3-from-a-data-scientist-whats-the-difference-between-first-party-and-third-party-data/>> accessed 14 June 2021
- Green A, 'Complete Guide To Privacy Laws In The US' (varonis, 4/2/2021) <<https://www.varonis.com/blog/us-privacy-laws/>> accessed 23 July 2021
- Heloise Walters, 'The state of cybersecurity in financial services' (Finextra, 28 May 2021) <<https://www.finextra.com/blogposting/20387/the-state-of-cybersecurity-in-financial-services>> accessed 27 August 2021
- Juliana De Groot, 'What Is GLBA Compliance? Understanding The Data Protection Requirements of the Gramm-Leach-Bliley Act In 2021' (Digital Guardian Tuesday July 6, 2021)<<https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act>> accessed 19 July 2021
- Kyra Kuik, 'How Can You Win Customer Trust and Be More Competitive?' (Siteimprove, Nov 14, 2019)<<https://siteimprove.com/en/blog/how-can-you-win-customer-trust-and-be-more-competitive/>> accessed 31 August 2021
- Maha Bahou, 'Where Does The Jordanian Financial System Stand On Open Apis?' (JOPACC 24.02.2020) <https://www.jopacc.com/EN/ListDetails/Blogs_Posts/20/2> accessed 18 June 2021
- Maha Bahou, 'Digital Identity: the missing link in Jordan's financial digitalization journey' (JOPACC 20.05.2020) <https://www.jopacc.com/EN/ListDetails/Blogs_Posts/20/5> accessed 18 June 2021
- Maxime Pallez, 'The Know-Your's-Third-Party Approach in Financial Services' (THE BLOG PWC 2020) <<https://blog.pwc.lu/the-know-your-third-party-approach-in-financial-services/>> accessed 17 July 2021
- Moayad Ghannam, 'Consumer Protection and Trust in Financial Services' (JOPACC 15.12.2020) >https://www.jopacc.com/EN/ListDetails/Blogs_Posts/20/8> accessed 18 June 2021
- 'Third Party Vendor Risk Management in the Banking Industry' (ERMProtect, 2021) <<https://ermprotect.com/blog/third-party-vendor-risk-management-in-the-banking-industry/>> accessed 10 July 2021
- 'What Is the Difference Between a Vendor and Third Party?' (Venminder January 29 2020) ><https://www.venminder.com/blog/differences-between-vendor-third-party>> accessed 16 June 2021
- Yaffa Klugerman, 'The 5 Most Notable Third-Party Data Breaches Of 2021 (So Far)' (Panorays Jul 22, 2021) <<https://www.panorays.com/blog/the-5-most-notable-third-party-data-breaches-of-2021-so-far/>> accessed 10 September 2021

Websites

- A Do'S And Don'Ts Guide For Lawmakers - Lessons From The EU General Data Protection Regulation To Contribute To The Global Discourse On Data Protection (Access Now 2018) <<chrome-extension://oemmnxcbldboiebfnladdacbfmadadm/https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>> accessed 11 June 2021

- Baker J, 'What Does the Newly Signed 'Convention 108+' Mean For UK Adequacy?' (Iapp.org, 2018) <<https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/>> accessed 23 July 2021
- 'Beyond GDPR: Data Protection around the World' (Thales Group, 2021) <<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world>> accessed 20 June 2021
- Carson a, 'Data Privacy Laws: What You Need to know in 2021' (Osano, July 20, 2021) <<https://www.osano.com/articles/data-privacy-laws>> accessed 23 July 2021
- 'Constitutional History of Jordan' (ConstitutionNet, 2021) <<https://constitutionnet.org/country/constitutional-history-jordan>> accessed 01 August 2021
- 'EPIC - The Right to Financial Privacy Act' (Epic.org, 2021) <<https://epic.org/privacy/rfpa/>> accessed 18 September 2021
- 'Financial Services And Legacy Systems: The Opportunity of Modernization | Mulesoft' (MuleSoft, 2021) <<https://www.mulesoft.com/resources/esb/financial-services-legacy-systems-modernization>> accessed 22 June 2021
- Flinders K, 'Digital Bank Customer Data Breached Through Third Party' (ComputerWeekly.com, 2021) <<https://www.computerweekly.com/news/252486767/Digital-bank-customer-data-breached-through-third-party>> accessed 10 September 2021
- Foitzik P, 'What You Must Know About 'Third Parties' Under GDPR and CCPA' (Iapp.org, 2019) <<https://iapp.org/news/a/what-you-must-know-about-third-parties-under-the-gdpr-ccpa/>> accessed 20 September 2021
- Karpilo J, 'Dividing The World Into The Haves And Have-Nots' (ThoughtCo, 2020) <<https://www.thoughtco.com/developed-or-developing-dividing-the-world-1434457/>> accessed 10 June 2021
- Meharchandani D, 'Third-Party Data Breaches: A Rising Threat' (Security Boulevard, 2021) <<https://securityboulevard.com/2021/06/third-party-data-breaches-a-rising-threat/>> accessed 10 September 2021
- 'Protecting Financial Consumer Data In Developing Countries: An Alternative to the Flawed Consent Model - UN Capital Development Fund (UNCDF)' (Uncdf.org, 2018) <<https://www.uncdf.org/article/3888/protecting-financial-consumer-data-in-developing-countries-an-alternative-to-the-flawed-consent-model>> accessed 9 June 2021
- Swinnen E, 'NGDATA | The Ultimate Data Privacy Guide for Banks and Financial Institutions' (NGDATA, 2020) <<https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/>> accessed 9 July 2021
- 'Sharing Personal Data with Law Enforcement Authorities' (Ico.org.uk, 2021) <<https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/>> accessed 12 July 2021
- 'The Finance Industry'S Guide to Marketing Data - Data Axle' (Data Axle, 2021) <<https://www.data-axle.com/resource/the-finance-industrys-guide-to-marketing-data/?download=true&id=5d7fab94-6aad-4c15-8b7c-4b242fdffdfa>> accessed 6 August 2021