Compliance Challenges with Personal Data Protection Laws in Big Data-Driven Fintech

Prepared by: Saja Abdulazeez , 20110060

Table of Contents

Table of Contents 2

I. Introduction: The Rise of Big Data 3

II. Literature Review 4

a. Questioning Ethics in Big Data Research 4

b. The Legal Angle of Data: Data Protection laws in the EU 5

Right to be forgotten 6

Data portability 7

c. The Legal Angle of Data: Data Protection Laws in Jordan 7

Big Data & AI in Fintech in Jordan 9

Digital Banking Customer Base in Jordan 9

III. Research Objective and Questions.. 10

IV. Research Methodology..11

Flowchart 13

Data Collection 13

Data Analysis 15

Data Findings 16

The need for Big Data technology 16

Personal Data , Access and Usage 16

Introduction of PDPL and its challenges 17

Data Governance, its aims and challenges... 18

Ethics, exploitation of big data 19

Customer trust and brand image 19

Summary and recommendations... 20

V. Conclusion.. 22

References.. 23

Appendix.. 25

I. Introduction: The Rise of Big Data

In a world where generative AI technologies have become the norm, spanning from chatbots and art generation to customer churn prediction and medical diagnoses, it is evident that this technology is on an upwards trajectory. Various industries are now, more than ever, recognizing the value and opportunities the digital age can bring. What fuels the uprising of this technology is the abundance of data surrounding us. “Each year we produce as much data as the entire history of humankind” (Helbing,2018). According to Statista (Taylor, 2023), **120 zettabytes of global data have been generated in 2023**, with expectations of a **150% increase by 2025**, sitting at 181 zettabytes. Of the data we generated this year, **76.27%** amounts of internet data traffic including a combination of videos, social media posts / text messages and gaming data – classified as **unstructured data**. This is where **big data** comes into play, deriving value from a plethora of unstructured, semi-structured (e.g. emails) and structured (e.g. tabular, organized) data. The goal is to leverage all types of data into a company asset, aiding our movement towards a data-driven culture.

Big data encompasses massive volumes of information that surpass traditional storage capabilities and processing tools, it demands cost-effective and innovative technologies. At its essence, big data involves the interlinkage and integration of large datasets from diverse sources, with an aim to derive valuable insights and knowledge (Schneble, 2022). This paradigm has found widespread applications in Telecommunication, Internet of Things (IoT), smart cities, cloud computing, financial services, healthcare, supply chain optimization, churn predictions, social media analytics.

This all-encompassing technology however comes with its challenges described as the 5 V’s: **Volume** – the sheer size of data and records being stored; we’ve now reached up to zettabytes (1000^7 bytes) even petabytes, *“1 million billion bytes”* (Helbing, 2018). **Velocity** – the speed at which data arrives mainly as streams, batches, or near real-time. **Variety** – the diversity of data types and sources. **Veracity** – refers to the accuracy and quality of data being stored and analyzed, if the data source is indeed credible and can be trusted. **Value** – I would argue the most important of the V's where we ask, *“does this data bring value to the organization?”* the answer is reached by proper data analytics to extract whether the data we have is insightful for data-driven decision making in the long run (Gutta, 2020).

The introduction of this technology opened many doors for innovation, in its complex yet intricate nature however, we stumble upon unexplored ethical, legal and implementation challenges when it comes to relying on this tech for insights and decision making. Given Jordan’s up and coming reliance on data and artificial intelligence one questions the readiness of the people and companies alike; with the introduction of the Personal Data Protection Law draft, The approaching years are set to bring challenges as we stand at the brink of a substantial departure from the norm.

Purpose Statement

“Exploring the Potential Technical and Non-technical Challenges Faced by Big Data Driven Organizations, Fintech Providers, in Jordan as a Result of Compliance to Personal Data Protection Laws”

II. Literature Review

The discussion of ethics and legal trade-offs in the field of Big Data Analytics (BDA) is in its infancy stage and is quite broad; there is no set-in stone system or standardized framework of the do’s and don’ts in BDA and AI. Globally however, there are some established “code of ethics”, or “code of conduct” generated by different organizations like the (1) IEEE *Ethics and Member Conduct*, (2) ACM *Code of Ethics and Professional Conduct*, and (3) Data Science Association *Code of Professional Conduct* that are derived from computer ethics (O’Leary, 2016). We also currently have data regulation laws such as the infamous European Union General Data Protection Regulation (GDPR); specifically article 6 which, broadly, is to ask the user for consent; yet we hear criticism of the GDPR as being law abiding but not easily understood by the average user; rarely would they take the time to read what they are “ticking themselves into” when joining online platforms or services (Elger, 2022).

So it’s simple, big data (BD) can be treated under the umbrella of those established codes of ethics and conduct mentioned above – no, actually it can’t, many argue it’s because of the nature of BD; the sheer complexity, volume and interlinkage between different data sources has created new challenges and raised ethical questions we haven’t seen before in regular data analytics (Wiltshire & Alvanides, 2022). The potential of big data is evident, and companies are eager to leverage this technology to grow at the pace of data and artificial intelligence in the realm of BD research, enabling enhanced services. However, the question remains: Are legal and ethical regulations able to keep up?

a. Questioning Ethics in Big Data Research

Here, we will explore the ethical implications of social media considering its reliance on big data technology, we can examine real-life situations where ethical considerations lagged behind advancements in big data research, so we can comprehend how ethics play a vital role in this field.

One notable case is the 2014 Facebook "emotional contagion" study, a large-scale A/B experiment involving the manipulation of news feed content by adding more negative posts. The aim was to observe the emotional impact on users, assessing whether it increased user engagement or led to expressions of anger. This study sparked significant controversy and raised ethical concerns because users were neither informed about their participation nor asked for consent to be part of this experiment (Metcalf and Crawford, 2016). The issue extends to the moment users sign up for Facebook and agree to *all* the terms and conditions, which, realistically, are rarely read by the average user. By checking that box, users unintentionally provide consent for their data to be used in Facebook's personal research and to be sold to 3rd parties(Shaw, 2022). These seemingly inconspicuous details accumulate over time, only becoming apparent when situations escalate beyond control.

Wiltshire & Alvanides (2022) mentions that BD is utilized by large retailer companies for targeted advertisements, this type of tech can be used to identify several demographics and influence them, it could fall into the wrong hands like political parties. An example of this is the 2016 Facebook – Cambridge Analytica "scandal". Zuckerberg was held in a trial before US congress in 2018 for selling personally identifiable data of around 87 million users (without informed consent) to Cambridge Analytica, a data firm that was later exposed to have targeted messages for the election of President Trump in the USA also known as "Project Alamo" (Isaak & Hanna, 2018), so predominantly being used for political advertising…propaganda if you will.

The data itself is not problematic, *"big data is ethically neutral"*. However it is ***how*** this data and technology are being used and to what ends would individuals go to in order to exploit the great potential that comes with big data innovation. This issue has created what Mark Andrejevic (2014) describes as "The Big Data Divide" which refers to the unstable relationship between those who collect, store and mine large quantities of data, and those who become the subjects of such data collection efforts (Christen, 2022).

b. The Legal Angle of Data: Data Protection laws in the EU

The intangible nature of big data in the boundless cyberspace challenges traditional laws and jurisdictions, it's common to observe the sale of anonymized data to third parties in exchange for monetary gain, particularly in Western cultures. In an effort to protect these data subjects against harm, the European Parliament (EP) introduced the general data protection regulations (GDPR) on April 14th, 2016, and went into effect on May 25th, 2018. GDPR aims to safeguard sensitive customer information – personally identifiable information (PII) against unauthorized access, misuse or disclosure. This regulatory framework informs EU organizations and those processing **any data of European citizens** on specific rules and regulations to appropriately store transfer and safeguard PII; meaning a global adherence to these regulations is expected (Stauber, 2018). Given a 2-year period to comply to these regulations before jurisdictions and consequences apply such as fines reaching up to 20 million euros or penalties up to 4% of all revenue generated by the company in that year, whichever is higher, it is safe to say companies must ensure strict adherence to these regulations to avoid legal, financial and brand image risks.

Remarkably, the compliance to GDPR was no easy task for majority of organizations, in a study conducted by Deloitte aimed to understand how a sample of organizations across Europe, Middle East and Africa were preparing for compliance in 2018 showed that **only 15%** of organizations surveyed to be **fully compliant by May 2018**, organizations have spent anywhere from **100,000 to 5M euros** in preparation for the new regulations. The reason behind this is many companies were obliged to change their entire IT infrastructure which required buying new hardware and licenses as well as hiring new staff and training current staff on new functionalities within the new infrastructure. Additionally, preparing employees for new roles such as a data privacy officer (DPO) (Stauber, 2018). These organizations mainly found challenges in these aspects of the GDPR:

Right to be forgotten

Article 17 of the GDPR officially names it as 'the right to erasure' meaning data needs to be deleted as soon as its fulfilled its purpose and is no longer needed while giving full authority to the data subject (the EU citizen) to have their data traces completely deleted; *'originally motivated by the desire of individuals not to be perpetually stigmatized by an action they did in the past'* (Abiteboul & Stoyanovich, 2019) ultimately the right to delete any traces they have on the internet to be completely forgotten, think of it like a clean slate. From the outside it seems very easy for companies to adhere to the right to erasure however (Mangini et al. 2020) states many challenges in doing so including data backups, deleting and tracing personal data from archives across an entire organization, especially if data is anonymized and encrypted, is a very labor and time-intensive task that must be done manually to trace the entirety of the data subject's information. A big data challenge intertwined with this aspect is if the company depends on the cloud rather than an on-premise data infrastructure, the organization needs close contact with the cloud service provider such as Azure or AWS to ensure the data subject's need is fulfilled and compliant by the GDPR to avoid penalties.

(Mangini et. Al 2020) 4 years after the introduction of GDPR; sought out a study that surveyed businesses including 50 respondents varying from senior management level to team leaders, about their difficulty in GDPR implementations. 87% of respondents surveyed Agree (4)-Strongly agree (6) to 'GDPR was a costly and difficult project' on the other hand 72% of correspondents felt that the GDPR introduced a great advantage to how personal data is being handled, so there is a trade-off observed between compliance – cost and advantages in the long run.

Data portability

In other words the right to receive personal data from a vendor, a data can then decide whether they want to delete their data or edit it ; the aim of this law is to empower individuals and provide information as to how their data is handled by preventing them from being overly reliant to a specific vendor's services. This adds competition between different vendors and gives the individual freedom of choice whether to continue with their service provider or choose another.

In data portability 'the devils in the details' (Abiteboul & Stoyanovich, 2019) there needs to be a stable and structured exportation of the data that allows it to be reusable by the parties asked for it, moreover a clear understanding of what and how data can be exported forms a challenge for IT experts such as deciding between the person's actual information, or the data created by the company upon that person's information. In the realm of big data this relates back to the data management (DM) / data governance (DG) framework an organization has in place, an absence in DG for any data driven organization makes the process of data flow and data portability a time consuming and difficult task, it aligns with the technical challenges stated for the right to be forgotten.

To sum up this section stressed the technical and non-technical challenges the GDPR imposed on organizations from secondary data across Europe organizations, that being said it raises some questions, introducing the draft of Jordan's Personal Data Protection Law (PDPL) can we see any similarities with the GDPR, and will compliance also raise challenges to big data-driven organizations in the kingdom? The next section discusses the similarities between the GDPR and PDPL.

c. The Legal Angle of Data: Data Protection Laws in Jordan

The Jordanian PDPL draft was published to the public by the Ministry of Digital Economy and Entrepreneurship (MoDEE) on September 17th, 2023, and will come into effect March 17th, 2024. The official draft is only available in Arabic, an initial scan of the laws shows very similar to the GDPR, from definitions of sensitive data, personal data to the overall structure of the laws. The PDPL states the penalties for non-compliance include firstly, a fine of 1000 – 10,000 JOD if any laws are breached and can be doubles in case of recurrence (Appendix Section 2). Secondly, cancellation or suspension of permits and licenses or a daily fine issued by the Personal Data Protection Board (PDPB) for each day a law is being violated no more than 500 JOD. Thirdly, the elimination of data or termination of a database that is associated with any case where a conviction order was issued. The regulatory body will issue a period to any non-compliant to rectify its violation, if the time period elapses with no corrections, the PDPB will incite any of the mentioned penalties as they see fit.

Verbatim, the PDPL includes the following data subject rights:

1. Rights of information, review, access to and obtaining of their personal data
2. The right to withdraw consent
3. The right to rectification, alteration, addition or updating of their data
4. The right to have their data processed for purposes falling within a specific scope
5. The right to erasure of data, i.e. the right to be forgotten under specific conditions in the law
6. The right to object to processing and profiling (handling and manipulating personal data and analyzing it such as categorizing based on characteristics and /or behavior) if these activities are no longer necessary, exceeded the requirements as the purposes of the data collected have been fulfilled, or if data subjects believe it is discriminatory, prejudicial, and law breaching
7. The right to transfer a copy of data
8. The right to be informed of any breach infringement or any data security and integrity breach.

A data subject should have the freedom to utilize these rights without experiencing any negative financial or contractual consequences. We can confidently state the PDPL and the GDPR share many similarities however tailored to each region, consequently we cannot jump to the conclusion that the challenges faced by European organization are similar to those in the Kingdom.

In an effort to narrow down this study, e-wallet / fintech providers were the focus of this proposal as the nature of the data being analyzed coincides with semi-structured and the amount of transactional data collected daily is massive. Another reason as to why fintech providers were chosen is because of the large Jordanian user base that has been steadily growing since COVID-19, the dependency on digital banking has gained popularity due to its convenience and banks across Jordan sought an opportunity to expand and gain more recognition. In the upcoming section, the dependency of big data technology in banks is discussed furthermore, a validation of the ever-expanding digital banking userbase in the Kingdom is mentioned.

Big Data & AI in Fintech in Jordan

During a seminar held in Al-Hussein Technical University guest speaker Eman Gammoh, Head of AI & Advanced Data Analytics at Arab Bank, a prominent data-driven customer-centric bank in Jordan, shared key insights regarding the bank's reliance on a robust big data platform. With over 600 branches spanning 5 continents, Arab Bank processes a vast amount of real-time data—approximately 18 million transactions across various channels. This data is meticulously analyzed to detect suspicious activities. Moreover, the bank employs clustering algorithms to create customer profiles based on purchase histories and transactional behavior, enabling them to better understand their customers and tailor services and loyalty programs accordingly.

Arab Bank has also implemented a customer churn prediction framework, recognizing the value of retaining existing customers rather than solely focusing on acquiring new ones. Additionally, sentiment analysis is employed to gain further insights from customer feedback, tweets, and financial news, aiding in the understanding of customer attitudes. These data-driven solutions consistently prioritize enhancing customer experience, offering personalized products and services, and driving targeted marketing initiatives.

Other global well-known banks that have implemented similar technologies include Bank of America, JP Morgan & Chase, Bank of China, HSBC, Bank of Canada, Wells Fargo (Gaol et al. , 2019) and in this fast-paced tech-driven society perhaps many more banks in the Kingdom. The use of BDA in Arab Bank allows them to gain a higher competitive advantage in the finance sector, and of course the same applies to other banks globally that utilize BDA. Financial data such as credit card information are deemed sensitive; customers are willing to share their data if they are confident in their bank’s ability to practice ethical management and protection of their data (Arthur & Owen, 2019). **Trust** and customer loyalty plays a crucial role in the current digital banking era.

Digital Banking Customer Base in Jordan

To further verify a dependency on fintech by the citizens of Amman, this section explores numbers shared by The Jordan Payments & Clearing Company’s Payment Systems Quarterly Report in July – August – September of 2023 (Q3) which states that the total number of CliQ (a special service that allows users to transfer money across different banks seamlessly and on the spot) **users** in Jordan is around **1014K**, 352.7K of these users are between the ages 18-30, their highest customer demographic. By September 2023 **8.6 million CliQ transactions were made** with a value of 1500 million JODs, **84% of those transactions were across different banks**. Another service and app operated by Madfoatcom is E-fawateercom where customers can conveniently and seamlessly pay for water & electricity bills, telecommunication services, governmental services, school / university tuitions and many more, the **total number of users** by

September 2023 is at **3.93M**, with a total number of **13.91M transactions 11M were digital** with a value of 2.97 billion JOD.

According to Ipsos, a global market research and consulting firm, released a paper on the Jordanian views on digital banking back in July 2023 (Elfar H. 2023) from a sample of **1000 respondents 43% have used digital banking channels with the majority being Gen Z and millennials**; the use of mobile banking applications increased 14% from 2022 and physically visiting a bank's branch decreased by 11%. 73% of respondents trust traditional banks whereas 42% trust payment processing companies.

These numbers verify that the userbase depending on fintech is not only large, but consistent given its convenient nature, we can conclude that majority of the users are generation Z (ages 18 - 27) and millennials (ages 28-43), majority of transactions are across different banks and are mainly digital – 11M of 13M transactions on E-fawateercom were digital. The dependency of digital banking is further validated by the decrease -11% of physically visiting the banks from 2022-2023. Finally, the majority of users trust traditional banks with digital services rather than payment processing companies or those that provide e-wallets.

III. Research Objective and Questions

Given the absence of current laws and regulations in Jordan concerning digital sovereignty, what legal and ethical challenges do big data-driven fintech providers face when creating customer-centric services, and how do these challenges impact data management and trust-building mechanisms with customers?

- To understand how big data frameworks and technologies are applied by data-driven fintech providers in Jordan.
- To comprehensively examine and evaluate the existing legal and self-regulatory (data governance) challenges faced by big data-driven fintech providers in Amman.

IV. Research Methodology

The majority if not all research studies require a specified approach and methodology to collect data which is essential for the validity and reliability of the data being collected, ensuring that it adheres to the research objectives. This allows for a consistent process applied by researchers to contribute credible findings across different settings and time periods. The two main approaches are qualitative or quantitative.

From a holistic perspective quantitative research quantifies relationships, behaviors and phenomena through numeric and statistical data analysis collected through questionnaires, surveys or existing data sets; it focuses on testing hypotheses and generalizing findings on larger populations. Through descriptive and inferential statistics researchers are able to find patterns, relationships, correlation, and predict outcomes. On the other hand, qualitative research emphasizes understanding complex meanings, the context behind interpreting a subjective experience relating to the research. Non-numerical approach often done through one-on-one interviews, focus groups or even observations which are analyzed through finding patterns or themes within the data collected. Qualitative approach focuses on the human experience uncovering a deeper social phenomenon to generate a theory. Some researchers approach a mixed approach applying both methods to get a comprehensive understanding and contribute valuable insights (Casebeer & Verhoef, 1997).

For this research proposal a qualitative approach is taken, collecting primary data through one-on-one interviews with experts in the field of big data and its use cases in their organizations. The reason behind a qualitative approach can be justified through Saunders Research Onion, developed by Saunders et al. in 2007, is a layered model, such that of an onion, that offers a detailed description of each stage of the research process. Layer by layer, a researcher is able to define the research philosophy, which research approach to be taken, which research strategy to adopt, the time horizon and the data collection methodology (Thesismind, 2019). The layers of the 'onion' are explored below with context to this research proposal:

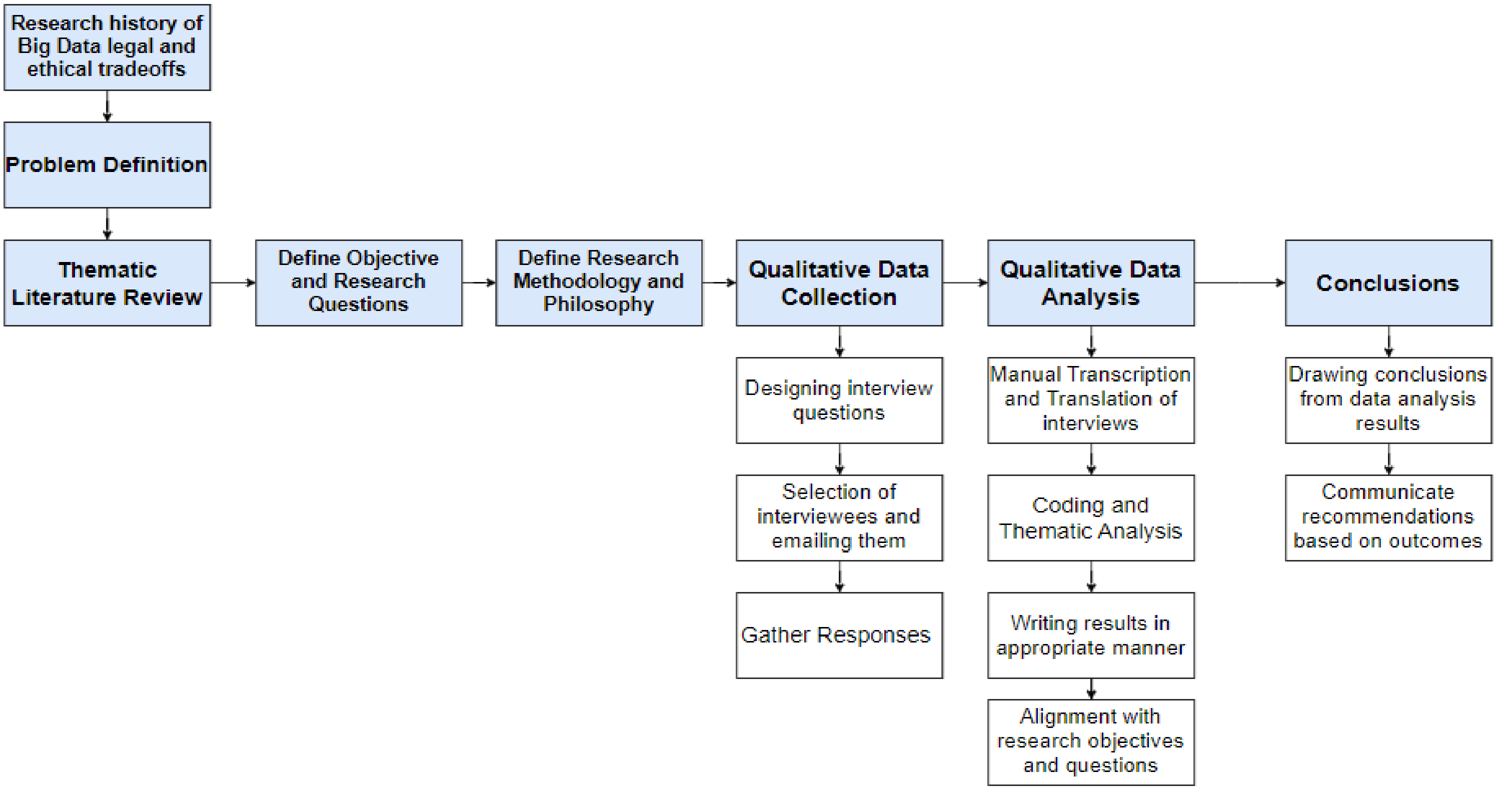
1. **Research Philosophy**: can be defined into two main philosophies; *positivism* – set in stone, facts based quantitative methods where a question or hypothesis can be tested such as scientific experiments evaluated and analyzed through detective logical reasoning, such as the discovery of the law of gravity, it is applicable on all people. The second philosophy is *interpretivism* – each individual has their own interpretation of something (an experience) depending on their own perception of reality utilizes qualitative methods, differing opinions and insights from one person to the other is gained. Unlike positivism it cannot be generalized. **Interpretivism is the philosophy followed here**, as each organization has its own set of values, goals, customers processes and use cases, the

challenges of company A does not align with those of company B or even to generalize for all companies in Jordan.

2. **Research approach**: Deductive approach includes developing hypotheses from a pre-existing theory, making predictions and experimenting just like scientific research which aligns with positivism philosophy. The inductive approach is to create a theory though observations, no initial framework is set however through data collection (primary and secondary) the focus of the research can be formed (Flick, 2011). It is commonly used for qualitative research and **in the case of this proposal** the approach was inductive where interviews were carried out regarding a specific phenomenon that is the introduction of PDPL will affect big data driven organizations in one way or another and from examining data, specific patterns were seen between respondents. Also through secondary data collection the objectives and questions of the research proposal were clarified.
3. **Research strategy**: how the researcher intends to carry out the data collection method through firstly, experimental – examining the results of an experiment against expected results. Secondly, through action to find a specific solution for a specific problem and is often applied in teaching or nursing. Thirdly, case study, which focuses on one or more people in a single area that can offer insights into the specified problem, comparing these experiences can establish key features and draw generalizations **which I believe aligns with the approach of my proposal**. Finally, surveys, linked with the deductive approach, are a simple and straightforward way to collect reliable data from a specific sample of people.
4. **Choice of method**: this can be Mono method, either qualitative or quantitative; mixed method, using both qualitative or quantitative such as interviews with experts in the field and collecting survey insights from a specified sample; or multi-method. **This proposal utilizes the Mono method qualitative.**
5. **Time horizon**: is the time frame within which the project is intended for completion, cross sectional – pre-established time framework where data must be collected or longitudinal – collection of data occurs multiple times with the same sample over years when the aim of the study is examine change overtime. **In the case of this proposal**, the time horizon was cross sectional, before the introduction of the by-laws by the MoDEE to examine what challenges companies are facing when preparing for compliance.
6. **Data collection and analysis**: the final layer is where justification of why and how the researcher undertook the research, the merits, limitations, ethical rules abided while utilizing both primary and secondary data, justifications for this are in the section ‘Data Collection’.

Flowchart

This flowchart covers the steps taken throughout the process of the creation of this research proposal:


Research history of Big Data legal and ethical tradeoffs
Problem Definition
Thematic Literature Review
Define Objective and Research Questions
Define Research Methodology and Philosophy
Qualitative Data Collection
Designing interview questions
Selection of interviewees and emailing them
Gather Responses
Qualitative Data Analysis
Manual Transcription and Translation of interviews
Coding and Thematic Analysis
Writing results in appropriate manner
Alignment with research objectives and questions
Conclusions
Drawing conclusions from data analysis results
Communicate recommendations based on outcomes

Data Collection

The data collected for this proposal incorporates both primary and secondary sources to address the research questions and objectives. **Primary sources** encompass any original material collected and analyzed at the outset of this research proposal, including recorded interviews conducted with experts in big data technology and data governance, with a focus on understanding the legal and ethical tradeoffs in the introduction of the Jordanian personal data protect laws (**PDPL**). Additionally, primary sources include official records such as cabinet papers, legislation, and case laws (Kemble W. , 2023). In this proposal these sources are the official published PDPL by the Jordanian Ministry of Digital Economy and Entrepreneurship (**MoDEE**) and the official European Union General Data Protection Regulations (**EU GDPR**).

Secondary sources refer to books or papers written and published by scholars worldwide that relate to the topic (Kemble W. , 2023), previously addressed in the literature review. The aim of utilizing secondary recourses is to gain a deeper understanding of the existing legal and ethical trade-offs in the context of big data, moreover, to clarify and provide context for the primary data collection process. Gaining insights from secondary sources allowed the research questions and objectives to take shape by identifying what current gaps exist in the realm of legal and ethical tradeoffs of big data here in Jordan. Ultimately, this proposal aims to bridge those existing gaps by collecting primary data and presenting recommendations.

Ethical rules abided in the context of this proposal include the safety and privacy of the interviewees, when reaching out to them a summary of the research objectives were given and the topic of big data ethical and legal tradeoffs. In every step **consent** was asked for to make sure that the interviewees allow for the interview to be recorded, they consented to their names and positions being shared in the proposal. Validating the interviewees that the recording will not be published anywhere and is purely for personal use to transcribe and analyze for the proposal.

The data was handled securely and manually (without the use of online transcription software or other thematic analysis software) to ensure the security and privacy of the data. The interviewees were aware of how their information will be used in the proposal. It was also clarified that the retention of this data will be securely deleted until the data has achieved its purpose in this proposal. The only person with **access** to the recordings is myself on my iPhone voice memos app, secured with a face ID and passcode; as well as access to the transcripts and any analysis done is also ensured through a passcode protected laptop.

One of the many **merits** of collecting data through interviews is the quality of the data. The face-to-face interviews allowed for the conversations to flow smoothly, deeply understand the context behind the interviewee, pick up on their social queues and fostered a space to ask more questions for clarifications on any missed points. Not only did it allow for new revelations in this proposal, but it enhanced my knowledge of the topic at hand.

Some of the **limitations** include that this process was quite time-consuming. Picking the right time and place to meet was a hassle, as some meeting places were somewhat far away. Another limitation included potential bias, where each person would speak on behalf of their experiences in their organizations but not from an overall, generalized view – what company A struggles with does not mean company B or all companies in Amman struggle with the same issues. The transcription was a tedious task, given our bilingual nature, many sayings were interpreted in Arabic; however, in analysis they were personally translated.

Not many tools were utilized in this process, no transcription or analysis software, only a recording device (personal phone) and note taking throughout the interview to refer back to the interview questions.

Data Analysis

The data analysis tool utilized was thematic data analysis manually following these main steps:

1. Taking notes during interview on points that aligned with research objectives
2. Listen to the recordings and transcribe the interviews verbatim (word for word)
3. Group and color code sayings with similar context
4. Generate initial codes
5. Generate and review initial themes
6. Name the themes
7. Produce report for analyzed data

The interview partners are:

Name	Background
Interviewee 1	Proficient background in Jordanian laws and regulations in regard to organizations and data, works closely with data engineers and data scientists to ensure data quality, taxonomy and privacy.
Interviewee 2	Lead data scientist, assistant manager in Data Science and AI – supporter of Neobank introducing tools such as anomaly detection and sentiment analysis as well as churn prediction.

Through emailing these experts in the field of big data / ML and data governance, mentioned in Appendix section 3 we were able to setup a meeting time and place, proceeding to ask for consent to record the interview for personal use when transcribing the voice recordings to proceed with thematic analysis; the intention for these recorded interviews were to understand the current legal and ethical landscape in Jordan with regards to utilizing big data for insights; the interviews were preferred to be face-to-face.

Data Findings

Through a specified set of questions aligning with the research objectives and questions (Appendix Section 4) were asked for the interviews, these questions were divided into 5 main topics:

1. Ice breaker to get to know the interviewees and their backgrounds
2. Validating a big data technology dependency in their organizations and the nature of personal data utilized (if any)
3. Their knowledge on the current legal landscape in Jordan with regards to the intangible nature of data and any issues / challenges faced by their organizations
4. Data governance (DG) and if the organization has this framework applied, and for what reasons was DG applied
5. Ethics and examples of unethical exploitation of big data
6. Customer communication and trust, how do they take consent from users and how utilizing their data is communicated

The generated themes through thematic analysis of the interviews are summarized in a appropriate manner below:

The need for Big Data technology

It's been determined that both organizations rely heavily on big data. Firstly, ML and AI models are constructed within a big data environment, enabling swift processing, particularly with vast amounts of transactional data. Secondly, the core of data-driven processes lies in identifying customer behavior through clustering algorithms. This allows for tailored campaigns and reward systems based on customer interests and preferred payment methods. Other algorithms include predicting customer churns, assessing risk scores, predicting the next best action (NBA) of a customer based on previous actions. Thirdly, the need for big data arises from traditional data warehousing environments' inability to handle large volumes and real-time data. Utilizing a hybrid cloud architecture streamlines daily operations, making them more efficient. Leveraging a big data platform allows for valuable insights to be extracted and utilized as a company asset rather than a burdensome overhead.

Personal Data , Access and Usage

The PDPL classifies personally identifiable data (PID) into **personal data** – anything that identifies a person, a full name, birthdate, national ID number, mobile number, location coordinates, a home address, card number; utilizing this type of data to assess customer behavior for research and development is often anonymized and occurs in bulks, there is no targeting on specific people. **Sensitive data** – include political interest, health, financial situation, race, sexual orientation which can be identified through the exploitation of a person’s data consumption and activity, with BD this can be a produced data set of the sensitive data. The utilization of personal data for research and development is covered under legitimate interest in the Jordanian law making it legal, it is not mentioned in the PDPL which is believed to create gaps in the law. Not to state the obvious its illegal however, under Jordanian law, to sell this data to third parties or to be done on sensitive data.

Personal data is given through the user themselves when signing up for a service, the majority of the data utilized is generated through different bank channels such as e-wallets or debit/credit transactions meaning full ownership of the data to the bank, they have every right to analyze for a customer centric approach. However, in the case of both organizations to ensure ethical use of personal data a thought-out data management framework is applied which identifies the individual responsibilities of employees within a company in regard to handling such data. Who has access to which data and for what reasons?, does a specific functionality truly depend on the access to personal data or not? Access isn't granted just to any random person there are specific protocols, NDAs and other legal papers to be signed that grant access to the PID. This is taken very seriously by both organizations as transactional data and financial data in general is considered under the umbrella of confidential information, additionally, regulations from the central Bank of Jordan must be abided.

Introduction of PDPL and its challenges

The initial draft of the data protection law was released back in September 2023 and includes many similarities with the GDPR and in March of 2024 the by-laws will be introduced which are clarifications for the initial laws. After the introduction of by-laws, organizations across Jordan have a 1-year probation period to allow companies to adjust to the new laws and prepare for compliance, compared to the EU GDPR 2-year probation period.

It was stressed that 1 year is a very short period to comply this is for a couple of reasons; changing the ways and procedures a company is used to after years requires consistent planning, applying new tools leading to more budget investments, hiring new experts and changing strategies, this includes applying a new IT architecture from a legacy and complex system to one that allows identification of PID and their storage inventory across the entire organization, and their corresponding branches.

The PDPL is demanding changing entire platforms to fulfill compliance for customer access, viewing and porting. The majority of companies today do not have the privilege of tracking a singular data entity for their own use, for compliance, creating a new platform from scratch is the go-to strategy.

The right to erasure of data was described as ‘a double-edged sword’ , thankfully in Jordan it's not for any individual but it is negotiable and case sensitive, it raised from the need for individuals to get a fresh start especially inmates who were applying to jobs, an employer would do simple google search and do a background check. In the sense of telecom, a telecom operator cannot delete billing data unless 10 years after the customer has churned which does not align with the right to be forgotten in the PDPL

A revelation has been reached where the introduction of the new laws will actually make operations more restricting for those working with data, in order for company people, law people, and average users to reach a maturity level on the PDPL will indeed be time consuming and requires thought out change management and planning.

The awareness of those with no background in IT or data does form a challenge as everything will be new and different; the lawyers do not have the competence of the details and complexities of IT systems but only on the surface level, they only refer to annexes which include any additional details to the case which could lead to more fines for non-compliance.

Lastly, the PDPL does not cover legitimate interest which allows organizations to provide the best of services through processing personal data, the organization should have access to do so to fulfill the requirements of the contract between a service provider and a customer; companies should have the space to generate revenues in an ethical manner all while providing to their customers campaigns and personalized services.

Data Governance, its aims and challenges

Data governance is a set of processes and policies framework that allows an organization’s use of its data in a beneficial manner, gaining them as an asset that enhances data-driven decision making, increase revenues and provide customers with better services. DG and legal departments work in parallel; to reach an ethical data-centric approach or organizational tasks to ensure standards are applied and laws and regulations and obliged with intensive monitoring and auditing ensuring no personal data has been leaked or used immorally.

Its aims are to modernize data systems with big data and to enhance the quality of data allowing a higher reliance on this data to bring value to the organization. Poor quality information can generate incorrect reports, inaccurate ML models, manual and heavy cleansing on data before report generation or model testing meant there was an inability to understand customer behavior rendering data ineffective and redundant.

The main challenge that was emphasized in applying DG vary from one company to another, but its essence is change management; it is difficult to change the mindset of employees who have been used to a specific way for a very long time, people are reluctant to change. This challenge aligns with the introduction of PDPL as some organizations in Jordan do not have a DG framework applied and as mentioned earlier, a demand to change full platforms to comply with the PDPL is inevitable.

It was highlighted that in Europe, countries including Slovakia, Belgium and Poland understand the risk of not complying with the GDPR however have chosen not to fully comply. They've decided it's more cost-efficient to pay fines rather than ensure 100% compliance with the GDPR. France and Spain to this day are struggling with full compliance since 2017 since all the laws are in theory and do not consider the sheer complexity of the IT systems especially, legacy companies.

Ethics, exploitation of big data

It was made clear that in the west, especially the USA, selling anonymized personal data in bulks to 3rd parties is quite normal such as Vodafone in Europe, they generate SMS ad campaigns for 3rd parties relying on their customers data. Majority if not all of the revenue generate by Facebook or Meta is from marketing social media campaigns on a specific targeted demographic, this is done with big data, Meta sells personal data, information, and behavior on their platform to third parties so that they can generate revenue; the ethical dilemma here is that you cannot use any Meta platform unless you accept all the terms and conditions, this relates back to (Elger, 2022) where users are unsure what they are 'ticking themselves into'

It was also highlighted that through big data exploitation sensitive personal data (political interests. sexual orientation, race) can be generated through personal data based on your data consumption and activity. In the context of AI models large language models such as ChatGPT are able to be broken, someone with a negative intent could convince the chatbot to do something unethical such as share sensitive personal data; if financial institutions are looking to apply LLM's they must make sure that their chatbot cannot be broken, if anything leaked even if it was a small incident financial institutions will not have the ability to recover especially in Amman where things like word of mouth is very aggressive and moves quickly.

Ensuring consent and brand image

Legacy banks here in Jordan have history relating back to 1950s, amidst crisis and war, every single customer retrieved every penny they owned which at the time no other bank was able to fulfill such task. This reputation dates into history and customers automatically gained the trust of this institution. Since then, this institution has put the effort into making this industry as customer centric as possible. As long as a customer is getting the expected service and more, trust is created.

Consent is a very crucial part of any digital banking services, as soon as a customer logs into an app, a pop up must take a yes or a no from the customer. UI designs ensure that the pop up cannot be removed by touching any part of the screen unless the answer is taken, if no consent is given the repercussions can be huge such as obtaining law suites, regulatory fines and other financial repercussions; additionally affecting the reputation of a company and potential loss of customers. Obtaining consent is covered under the PDLP and under the central bank of Jordan.

Summary and recommendations

These findings answer the set objectives, firstly, it is highlighted that there is indeed a reliance on big data technologies in digital banking companies in Jordan with a focus on running ML/AI algorithms seamlessly, streamline the flow and processing of tremendous amounts of near-real time transactional data , enrich data-driven decision making based on customer behavior and ultimately enforce a customer centric approach to create and elevate digital banking services.

Secondly, a clarification on personal data is provided as well as the practices and protocols followed by organizations when handling accessing and processing such data. Thirdly, the existing legal regulations in Jordan were further understood and in what ways they effect organizational process ranging from technical to employee level change management. The challenges highlighted are:

- **Challenge:** The 1-year probation period set by the law to prepare for compliance is very short, compared to the 2 years given for the GDPR.
    - **Recommendation:** It is recommended to extend the probation period and offer by-laws that further clarify the laws.
- The PDPL is demanding complete changes in platforms organizations have had in place for years
    - It is recommended for companies to work hand in hand with IT consulting services, preferably European, to prepare for PDLP compliance to hopefully avoid massive budget cuts.
- During the 1-year period, organizations are expected to invest in new tools, upgrade current IT architecture (if necessary), changing set-in-place strategies, hire new experts for new positions such as data protection officer (DPO) and auditors to ensure steady compliance with the PDPL and in general create substantial investments to avoid fines and revocation of licenses or data bases.

    - A critical analysis and study of the PDPL must be done by the organization’s Data governance / management team and law departments working hand in hand with the rest of the departments, if no law department exists then outsourcing such services is possible. A clear understanding of the organization’s ‘ins and outs’ must be made clear and transparent especially of the data flow, it is also wise to ensure compliance by holding monthly audits on the infrastructure and which departments and individuals have access and utilization to personal data.
- Raising awareness and reaching a level of maturity of the PDPL to those with no background in IT such as lawmakers and citizens alike will require years and a lot of patience.
    - There is no specific recommendation other than **time**, a crucial aspect that can either make or break the introduction of PDPL and is a shared event for organizations, lawmakers, staff and citizens alike.
- Employees are reluctant to change the established office practices, infrastructure and workflows which they have grown accustomed to over the years.
    - Change management should be at the front of preparing for compliance or if an organization does not have an established data management framework, a gradual introduction to the new workflows can help mentally prepare employees for changes and more importantly, great leadership practices by team leaders and directors should keep in mind the wellbeing of their employees while simultaneously running the company as usual to ensure continuity of services to customers.
- The PDPL does not cover legitimate interest – which lawfully allows companies to utilize anonymized personal data for legitimate purposes such as fraud prevention or manage accounts without explicit consent – creating gaps in the regulations as to **how** companies are allowed to utilize personal data.

The challenges mentioned above align with the challenges collected from secondary resources on GDPR and European organizations mentioned in the literature review which can be considered by Jordanian established organizations to aid them in preparing for compliance, the primary data however includes the human factor of employees, citizens and lawmakers as well as the absence of legitimate interest which is in fact mentioned in Article 6 of the EU GDPR.

Fourthly, the definition, needs and aims of self-regulatory means (data governance) were highlighted as well as the unethical exploitation of big data technologies by large and well-established western corporations. Finally, the level of trust between BD-driven organizations and customers was emphasized, more specifically how organizations ensure taking consent from users is mandatory, the use of their data clearly communicated through terms and conditions, and how focused these Jordanian organizations are on putting customers well-being at the forefront.

V. Conclusion

In conclusion, the integration of Big Data technology is essential for organizations, facilitating swift processing of vast amounts of transactional data and enabling the construction of machine learning and artificial intelligence models. However, the ethical and regulatory challenges surrounding the use of personal data underscore the importance of robust data governance frameworks and adherence to data protection laws such as the Personal Data Protection Law (PDPL) in Jordan. Implementing effective data governance practices is crucial for enhancing data quality, ensuring compliance, and fostering ethical data usage within organizations. Despite challenges such as resistance to change and complexity of IT systems, prioritizing transparency and obtaining explicit consent from users are vital steps in building and maintaining customer trust.

In summary, while Big Data technology offers opportunities for innovation and growth, it requires a balanced approach that considers ethical considerations, regulatory compliance, and customer trust. By addressing these challenges proactively and implementing robust data governance frameworks, organizations can maximize the benefits of Big Data while upholding individuals' rights to privacy and data protection.

References

- Helbing, D. (2018) ‘Societal, economic, ethical and legal challenges of the Digital Revolution: From Big Data to deep learning, artificial intelligence, and manipulative technologies’, *Towards Digital Enlightenment*, pp. 47–64. doi:10.1007/978-3-319-90869-4_6.
- Taylor, P. (2023) *Data Growth Worldwide 2010-2025*, *Statista*. Available at: https://www.statista.com/statistics/871513/worldwide-data-created/ (Accessed: 14 November 2023).
- Viganò, Eleonora and Christen, Markus and Elger, Bernice S. and Ienca, Marcello and Loi, Michele and Schneble, Christophe and Burri, Mira and Hauser, Christian and Shaw, David, Ethical, Legal and Social Issues of Big Data - A Comprehensive Overview (April 11, 2022). White Paper of the ELSI Task Force for the National Research Programme “Big Data” (NRP 75), Available at SSRN: https://ssrn.com/abstract=4081192
- Gutta, S. (2020) *The 5 V’s of big data*, *Medium*. Available at: https://medium.com/analytics-vidhya/the-5-vs-of-big-data-2758bfcc51d (Accessed: 14 November 2023).
- D. E. O'Leary, "Ethics for Big Data and Analytics," in IEEE Intelligent Systems, vol. 31, no. 4, pp. 81-84, July-Aug. 2016, doi: 10.1109/MIS.2016.70.
- Wiltshire, D. and Alvanides, S. (2022). Ensuring the ethical use of Big Data: lessons from secure data access. *Heliyon*, 8(2), p.e08981. doi:https://doi.org/10.1016/j.heliyon.2022.e08981.
- Metcalf, J. and Crawford, K. (2016) ‘Where are human subjects in Big Data Research? the emerging ethics divide’, *Big Data & Society*, 3(1), pp. 1–2. doi:10.1177/2053951716650211.
- Isaak, J. and Hanna, M.J. (2018) ‘User Data Privacy: Facebook, Cambridge Analytica, and privacy protection’, *The Policy Corner*, 51(8), pp. 56–57. doi:10.1109/mc.2018.3191268.
- Andrejevic, M. (2014). Big Data, Big Questions| The Big Data Divide. *International Journal of Communication*, [online] 8(0), p.17. Available at: https://ijoc.org/index.php/ijoc/article/view/2161.
- Stauber, S. (2018). *Compliance issues within Europe’s General Data Protection Regulation in the context of information security and privacy governance in Swedish corporations*. [online] Available at: https://www.diva-portal.org/smash/get/diva2:1213490/FULLTEXT01.pdf.
- Deloitte (2018). *Deloitte GDPR Benchmarking Survey: The time is now* . [online] Deloitte Georgia. Available at: https://www2.deloitte.com/ge/en/pages/risk/articles/deloitte-gdpr-benchmarking-survey-the-time-is-now.html.
- Abiteboul, S. and Stoyanovich, J. (2019). Transparency, Fairness, Data Protection, Neutrality. *Journal of Data and Information Quality*, 11(3), pp.1–9. doi:https://doi.org/10.1145/3310231.
- Mangini, V., Tal, I. and Moldovan, A.-N. (2020). An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective. *Proceedings of the 15th*

International Conference on Availability, Reliability and Security. doi:https://doi.org/10.1145/3407023.3407080.

- Wilkinson, D., Bajunaid, L. and Ooijevaar, M. (2023b). *Jordan issues first personal data protection law : Clyde & Co*. [online] www.clydeco.com. Available at: https://www.clydeco.com/en/insights/2023/10/jordan-issues-first-personal-data-protection-law.
- Indriasari, E., Gaol, F.L. and Matsuo, T. (2019). Digital Banking Transformation: Application of Artificial Intelligence and Big Data Analytics for Leveraging Customer Experience in the Indonesia Banking Sector. *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*. doi:https://doi.org/10.1109/iiai-aai.2019.00175.
- Arthur, K.N.A. and Owen, R. (2019). A Micro-ethnographic Study of Big Data-Based Innovation in the Financial Services Sector: Governance, Ethics and Organisational Practices. *Journal of Business Ethics*, 160(2), pp.363–375. doi:https://doi.org/10.1007/s10551-019-04203-x.
- JoPACC. (2023). *Payment Systems Quarterly Report*. [online] Available at: https://www.jopacc.com/sites/default/files/2023-10/q3_systems_2023.pdf.
- Elfar, H. (2023). *Views On Digital Banking in Jordan*. [online] Ipsos Jo. Available at: https://www.ipsos.com/en-jo/views-digital-banking-jordan#:~:text=Jordanian%20customers%20are%20increasingly%20turning,confidence%20towards%20nontraditional%20financial%20providers.
- Verhoef, M.J. and Casebeer, A.L. (1997). Broadening horizons: Integrating quantitative and qualitative research. *The Canadian Journal of Infectious Diseases*, [online] 8(2), pp.65–66. doi:https://doi.org/10.1155/1997/349145.
- Thesismind (2019). *Analysis of Saunders Research Onion*. [online] Thesismind. Available at: https://thesismind.com/analysis-of-saunders-research-onion/.
- Flick, U. (2011). Introducing research methodology: A beginner's guide to doing a research project
- Kemble, W. (2023). *Research guides: UTSC Finding Primary Sources: Home*. [online] guides.library.utoronto.ca. Available at: https://guides.library.utoronto.ca/utsc_primarysources.

Appendix

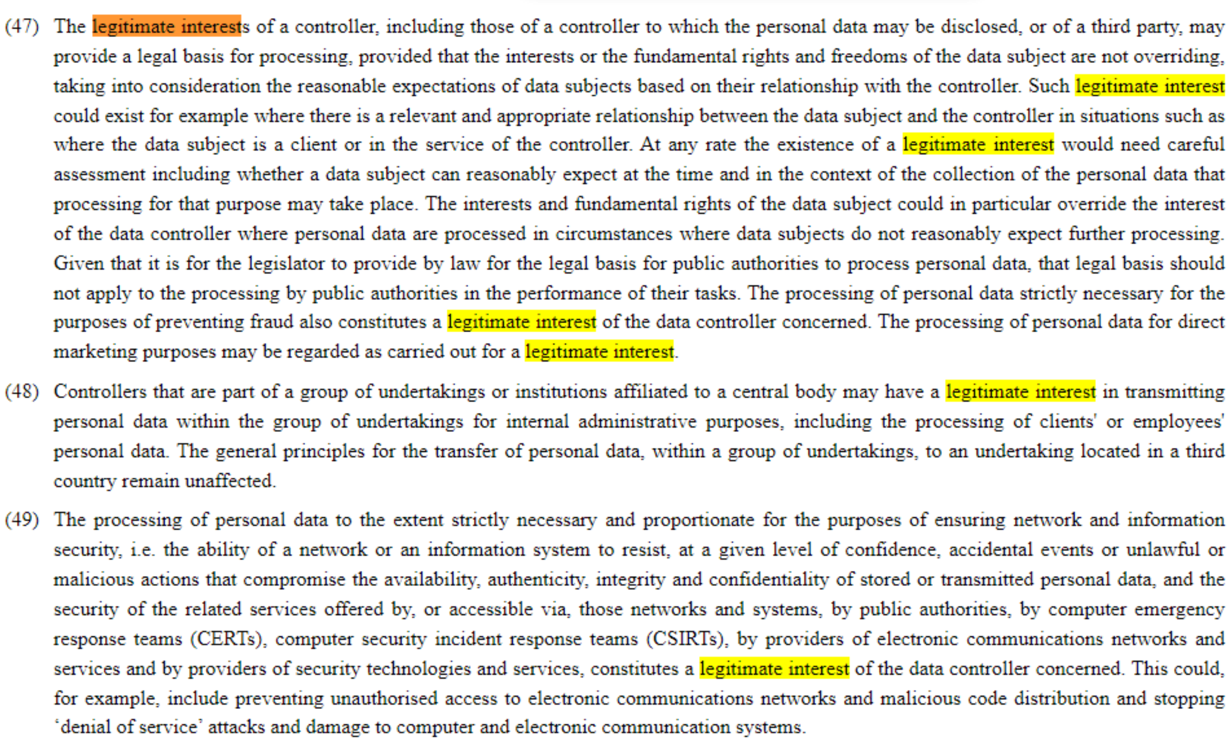
1. The European Union General Data Protection Regulations:

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 6 of the GDPR in detail clarifying the basis for legitimate interest



(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Rights of the data subject

Section 1Transparency and modalities

Article 12Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2Information and access to personal data

Article 13Information to be provided where personal data are collected from the data subject

Article 14Information to be provided where personal data have not been obtained from the data subject

Article 15Right of access by the data subject

Section 3Rectification and erasure

Article 16Right to rectification

Article 17Right to erasure (‘right to be forgotten’)

Article 18Right to restriction of processing

Article 19Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 20Right to data portability

Section 4Right to object and automated individual decision-making

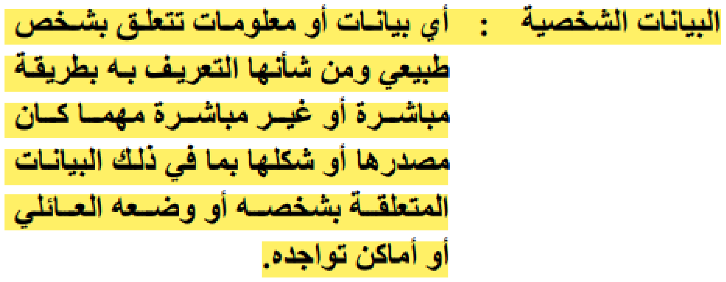
Article 21Right to object

Article 22Automated individual decision-making, including profiling

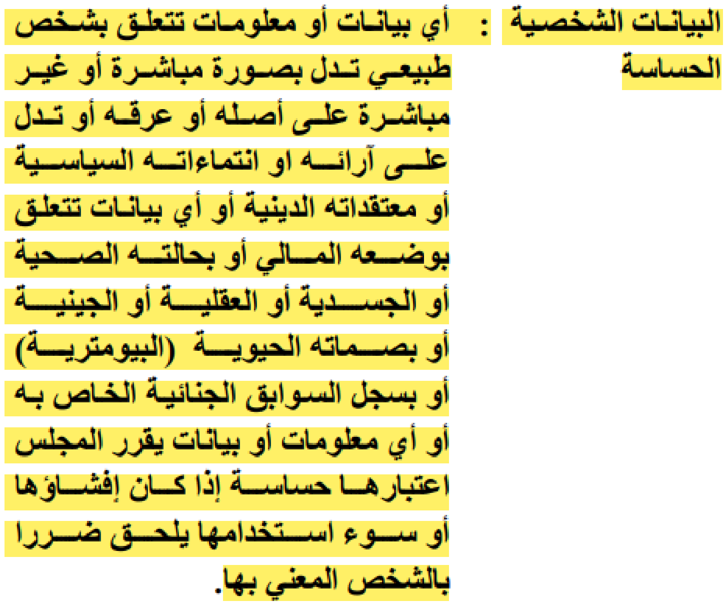
Section 5Restrictions

Article 23Restrictions

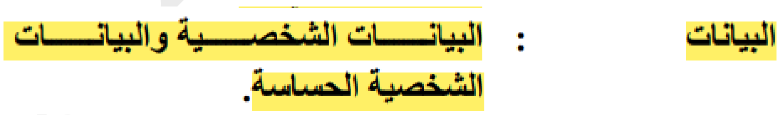
2. The Jordanian Personal Data Protection Laws by the Ministry of Digital Economy and Entrepreneurship:
   Definitions:



البيانات الشخصية : أي بيانات أو معلومات تتعلق بشخص
طبيعي ومن شأنها التعريف به بطريقة
مباشرة أو غير مباشرة مهما كان
مصدرها أو شكلها بما في ذلك البيانات
المتعلقة بشخصه أو وضعه العائلي
أو أماكن تواجده.

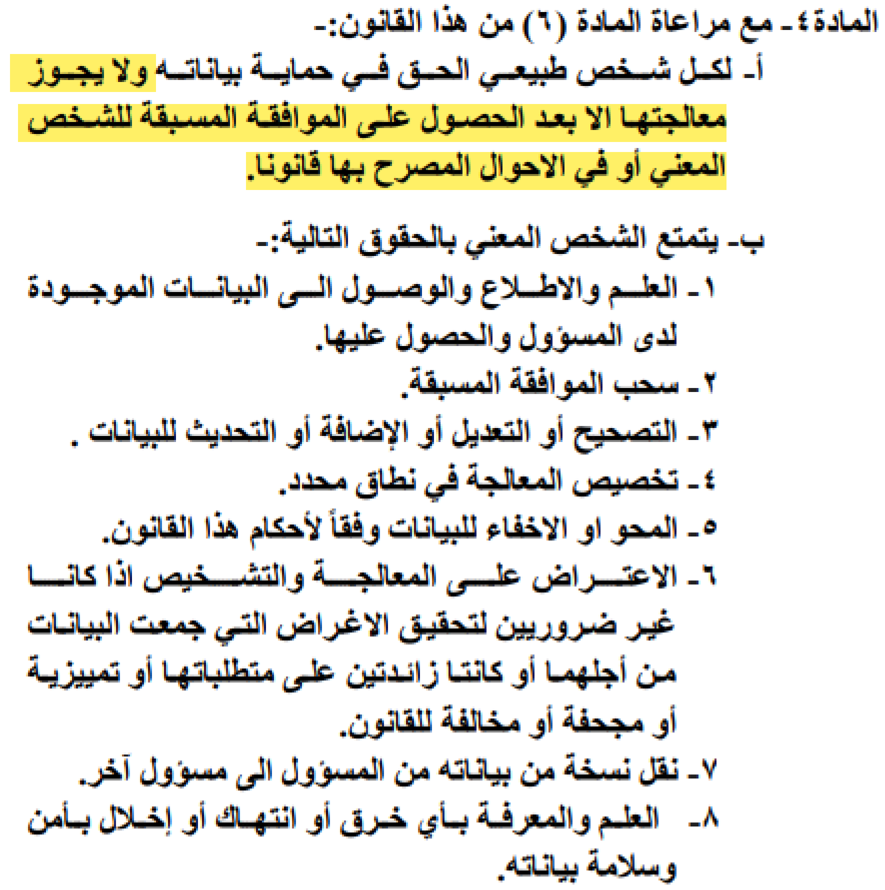


البيانات الشخصية : أي بيانات أو معلومات تتعلق بشخص
الحساسة طبيعي تدل بصورة مباشرة أو غير
مباشرة على أصله أو عرقه أو تدل
على آرائه او انتماءاته السياسية
أو معتقداته الدينية أو أي بيانات تتعلق
بوضعه المالي أو بحالته الصحية
أو الجسدية أو العقلية أو الجينية
أو بصماته الحيوية (البيومترية)
أو بسجل السوابق الجنائية الخاص به
أو أي معلومات أو بيانات يقرر المجلس
اعتبارها حساسة إذا كان إفشاؤها
أو سوء استخدامها يلحق ضررا
بالشخص المعني بها.



البيانات : البيانات الشخصية والبيانات
الشخصية الحساسة.

Data subject rights:



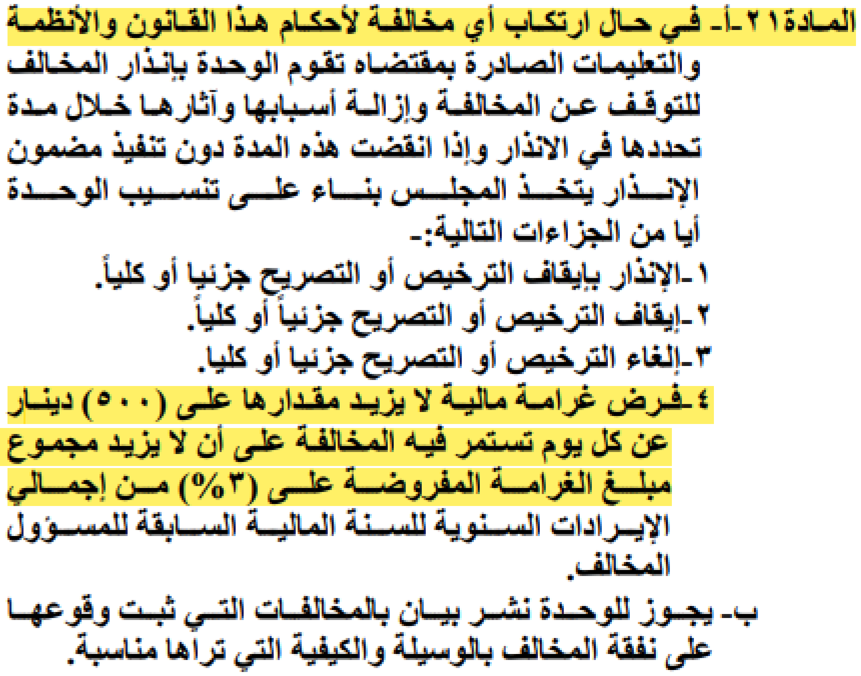
المادة٤ـ مع مراعاة المادة (٦) من هذا القانون:ـ

أ- لكل شخص طبيعي الحق في حماية بياناته ولا يجوز معالجتها الا بعد الحصول على الموافقة المسبقة للشخص المعني أو في الاحوال المصرح بها قانونا.

ب- يتمتع الشخص المعني بالحقوق التالية:-

١- العلم والاطلاع والوصول الى البيانات الموجودة لدى المسؤول والحصول عليها.
٢- سحب الموافقة المسبقة.
٣- التصحيح أو التعديل أو الإضافة أو التحديث للبيانات .
٤- تخصيص المعالجة في نطاق محدد.
٥- المحو او الاخفاء للبيانات وفقاً لأحكام هذا القانون.
٦- الاعتراض على المعالجة والتشخيص اذا كانا غير ضروريين لتحقيق الاغراض التي جمعت البيانات من أجلهما أو كانتا زائدتين على متطلباتها أو تمييزية أو مجحفة أو مخالفة للقانون.
٧- نقل نسخة من بياناته من المسؤول الى مسؤول آخر.
٨- العلم والمعرفة بأي خرق أو انتهاك أو إخلال بأمن وسلامة بياناته.

Legal consequences and penalties:



المادة٢١-أ- في حال ارتكاب أي مخالفة لأحكام هذا القانون والأنظمة والتعليمات الصادرة بمقتضاه تقوم الوحدة بإنذار المخالف للتوقف عن المخالفة وإزالة أسبابها وآثارها خلال مدة تحددها في الانذار وإذا انقضت هذه المدة دون تنفيذ مضمون الإنذار يتخذ المجلس بناء على تنسيب الوحدة أيا من الجزاءات التالية:-

١-الإنذار بإيقاف الترخيص أو التصريح جزئيا أو كلياً.
٢-إيقاف الترخيص أو التصريح جزئياً أو كلياً.
٣-إلغاء الترخيص أو التصريح جزئيا أو كليا.
٤-فرض غرامة مالية لا يزيد مقدارها على (٥٠٠) دينار عن كل يوم تستمر فيه المخالفة على أن لا يزيد مجموع مبلغ الغرامة المفروضة على (٣%) من إجمالي الإيرادات السنوية للسنة المالية السابقة للمسؤول المخالف.

ب- يجوز للوحدة نشر بيان بالمخالفات التي ثبت وقوعها على نفقة المخالف بالوسيلة والكيفية التي تراها مناسبة.

3. Interviewees emails / messages when contacted:

Email to interviewee 1:

*‘Good morning Dr. ***** , I hope this email finds you well*

As the subject of this email suggests, I would like to ask your guidance in my project; Big Data legal and ethical tradeoffs, my research question is as follows:

"Given the absence of current laws and regulations in Jordan concerning digital sovereignty, what legal and ethical challenges do big data-driven banks face when creating customer-centric services, and how do these challenges impact data governance, ethical standards, and trust-building mechanisms in the development of digital banking services?"

I recall in one of our Big Data lectures, a guest speaker (a colleague of yours) gave us an overview of data governance, if I may get her info so I can schedule an interview since I believe she is very competent in this subject and could help me reach valuable insights on this topic in regard to Jordan.

Through these interviews I aim to validate the big data divide which is "the unstable relationship between those who collect, store and mine large quantities of data, and those who become the subjects of such data collection efforts" moreover, to evaluate the existing legal, ethical, and self-regulatory challenges faced by big data-driven corporations in Amman as they leverage personal data for the development of customer-centric services and enhanced user experiences.

Thank you for your time.

Best Regards,

Saja Abdulazeez’

‘Good morning and a happy new year!

thank you for taking the time to go over my request for an interview, my schedule is free on these dates:

- *Saturday Jan. 6th*
- *Monday Jan 8th*
- *Tuesday Jan 9th*

I'll leave it up to you to decide the time and place depending on your schedule and I personally prefer face to face. Our interview could take around 45 minutes (maybe more) just to let you know.
*if you have any questions don't hesitate to email me or WhatsApp me on 0790******

thank you for your time.'

Message to interviewee 2:
*'Good morning Ms. **** ,*
Hope you're doing well. I'm Saja Abdulazeez a 4th year information science student and I had the privilege of attending your seminar at our uni a few weeks ago. I'm conducting research on the legal and ethical tradeoffs of big data tech in digital banking with a focus on enhanced customer experience in Jordan.
I would be honored to interview you as an expert in the field, especially considering Arab Bank's reliance on a big data framework, your insights are valuable to me and my research could you please share your availability and preferred location for the interview? I'm flexible and can adjust to your schedule; here are some suggested dates:
- Thursday, Jan 4th
- Saturday, Jan 6th
- Monday, Jan 8th
thank you so much for considering my request, looking forward to hearing from you.
Happy New Year's Eve!'

4. Interview Questions:

Introduction to the topic and ice breaker to get to know the interviewee and their background

Big Data Dependency, Utilization and Personal data use:

- Does your organization rely on big data applications (BD tech / frameworks) for its operations?
- If so, could you elaborate in which areas and how it is employed?
- In the context of your organization how do you define and identify 'personal data'?
- To what extent does your organization utilize such personal data for research and development purposes? (to create / enhance customer services?)

Legal landscape and challenges in Amman Jordan:

‘Given the intangible nature of data, it is challenging traditional laws on jurisdiction, and we see many companies today recognizing the value behind data’

- Since you’re an expert in this field; could you explain to me what the current landscape on data / personal data looks like for data driven organization here in Amman?
- In the perspective of legality and ethics, were there challenges your organizations faced to get to where they are today given the lack of digital sovereignty in Jordan?
- In your words how can we enhance the current laws on jurisdiction in regards to data here in Jordan?
- Does your organization adhere to any data protection law regulations like the EU GDPR?
- How does your organization today approach ethical decision making when utilizing customer data for research and development?

Data Governance:

- Could you explain to me, if your organization has a data governance / management framework, what exactly is DG and what problems did it serve solutions for in the context of your organization
- So why did your organization decide to establish DG, was it a self-regulatory decision or based on external factors?
- Could we enhance DG so that it involves legal and ethical dilemmas that data governance organizations face?

Customer communication and trust:

- When we speak of your organization we see that many people are trusting and confident of your services, in your opinion how did your organization reach this level?
- Do you believe users are concerned about their privacy and the security of their personal data or is that not an issue here in Amman?
- Do you inform your customers beforehand that their personal data will be utilized and if so, what are the procedures?

Reflections:

- how would you rate this interview and do you have any extra thoughts you would like to add?