A black and white logo

Description automatically generated

Complying with the Jordanian Data Protection Law

Contents

[Overview of Jordanian General Data Protection Law 2](#_Toc156229248)

[Introduction to Metropolis 3](#_Toc156229249)

[Mapping Sensitive Data for Compliance with Jordanian Data Protection Standards 3](#_Toc156229250)

[The Critical Importance of Data Protection for Corporate Integrity 3](#_Toc156229251)

[Can we say that any Personal data is Sensitive data 4](#_Toc156229252)

[Figure1: Complying with ISO and The Jordanian law for protecting the data 4](#_Toc156229253)

[Metropolis Asset Inventory 6](#_Toc156229254)

[6](#_Toc156229255)

[Figure2: Simplified Example on the Data Assets 6](#_Toc156229256)

[Figure3: Simplified Network Diagram that represent the Metropolis Subnets 7](#_Toc156229257)

[What is the role for the Data Controller and the Data processor within the domain of Metropolis 8](#_Toc156229258)

[Data Collector Responsibilities: 8](#_Toc156229259)

[Data Processor Responsibilities: 10](#_Toc156229260)

[Risk Assessment 10](#_Toc156229261)

[Data Subject Rights 12](#_Toc156229262)

[Right To Access: 12](#_Toc156229263)

[Right To Rectification: 12](#_Toc156229264)

[Right To be Forgotten: 12](#_Toc156229265)

[Right To Data Portability: 12](#_Toc156229266)

# Overview of Jordanian General Data Protection Law

The document provides a comprehensive overview of personal data protection laws and procedures, focusing on rights, responsibilities, and regulatory aspects. At the beginning it focuses on different definitions and how those terms might differ from organization to another based on its processes and Environmental Infrastructure, first it defines the difference between both the sensitive data and the personal data and some of the cases in which the personal data might be encountered as sensitive data, by this is claims that to comply we have to categorize or classify the assets if they are either sensitive or personal data.

Then, represents the difference between Data controller and the data processor by representing that the Data controller is the entity that is responsible for determining why and how personal data is processed. They are largely in charge of verifying that data processing is legal. They must develop data processing rules and guarantee that personal data is treated legally, fairly, and transparently, while protecting the rights and privacy of the persons involved. The Data Controller is ultimately liable for any data breaches and must guarantee that all required security measures to secure the data are in place. While the Data Processor, is the entity handles personal information on behalf of the Data Controller. They are responsible for managing the data in accordance with the Controller's instructions and must guarantee that their handling is safe and secret. They do not make choices concerning data processing operations; instead, they carry them out in accordance with the Controller's instructions. Processors have less autonomy and are directly involved in the practical side of data processing, such as data storage, retrieval, or IT assistance.

The text outlines specific steps for persons to follow to exercise their rights. Data controllers and processors must get legal consent and treat data in a legitimate way, considering the data's sensitivity and confidentiality. The statement calls for the formation of a Council for the Protection of Personal Data, which would oversee monitoring compliance, addressing complaints, and advising data controllers and processors.

Personal data protection is about more than just compliance; it is also about trust and ethical treatment of individuals' information. The paper recognizes the importance of personal data in the digital economy and attempts to develop a balanced legal framework that respects individual rights while facilitating data processing and innovation. The legislation intends to build a culture of privacy respect by providing explicit standards and requirements, as well as to contribute to the responsible growth of digital services and trade.

# Introduction to Metropolis

Metropolis Transit is a new corporation managing regional transit for a large metropolitan area, that operates in transportation business. Due to the importance of the data either if it was for the employees or for the customers to be protected in all its forms, transmitted, stored, collected and when processed. The company recognizes the importance of safeguarding personal data and ensuring compliance with data protection laws.

# Mapping Sensitive Data for Compliance with Jordanian Data Protection Standards

Sensitive data for a company like Metropolis typically includes types of information that, if disclosed or used without authorization, could cause significant harm or risk to individuals or the organization itself, in the context of Metropolis Transit, a company likely dealing with a large volume of passenger data and operating within a specific legal framework.

# The Critical Importance of Data Protection for Corporate Integrity

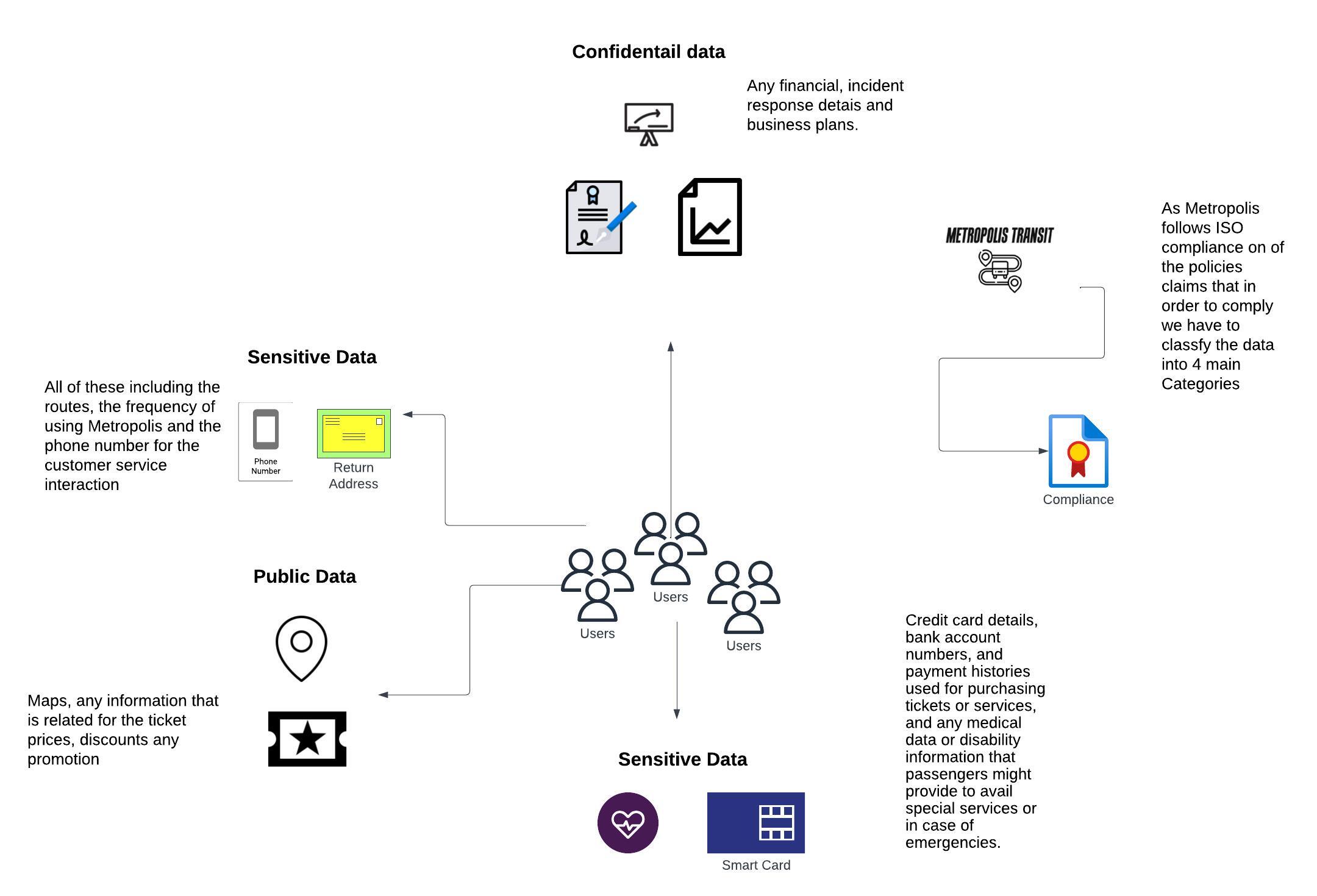
Understanding and categorizing sensitive data is crucial for Metropolis Transit for various reasons, including compliance with data protection legislation, retaining passenger confidence, guaranteeing safety and security, and enhancing service delivery. Not only must the firm identify these categories of data, but it must also develop effective security procedures and policies to manage and secure them, ensuring they are treated correctly throughout their lifespan, from collection to disposal.

When data such as PII, which is any information that identifies the passenger such as name, email, and maybe image, is leaked, it can result in loss of consumer trust, unfavorable media attention, legal ramifications, and, ultimately, a ruined reputation. A data breach may have serious consequences for a corporation like Metropolis Transit, which relies on public confidence and reputation to recruit and keep consumers. Customers may be hesitant to utilize the service if they perceive their personal or financial information is at risk, perhaps resulting in a company loss. Furthermore, regaining public trust following a breach may be a time-consuming and costly process that involves better security measures, public relations efforts, and, in some cases, legal settlements or fines.

# Can we say that any Personal data is Sensitive data

Relatable for Metropolis there is a difference between sensitive data and the personal data, as it is claimed that Metropolis follows the ISO standardization and to comply with we must ensure on the compliance that is achieved by Data classification that Metropolis Categorize the data into 4 categories not only the Personal and the sensitive data.[..\Lab 1\Enterprise Policy.docx](../Lab%201/Enterprise%20Policy.docx)

Adding to that, that Personal data refers to any information related to an identifiable individual. It's the broader category under which sensitive data falls. This information can be used on its own or with other data to identify, contact, or locate a single person, On the other hand, Sensitive data is a subset of personal data that, due to its nature, has been classified as requiring stricter handling and protection measures. It's generally the type of data that could lead to significant harm to an individual's privacy or wellbeing if disclosed or accessed without authorization.



## Figure1: Complying with ISO and The Jordanian law for protecting the data

As the graph represent an overview of Metropolis Data classification as specified above in the Enterprise policy, Certain types of personal data are inherently more sensitive due to the potential impact on an individual's privacy and wellbeing. For example, while a passenger's name is personal data, their financial information or health details are inherently more sensitive because unauthorized access could lead to financial theft, discrimination, or personal distress.

adding to that that it differs between the Sensitive and personal data, by in some circumstances the way personal data is used in providing services can make it sensitive. For instance, travel patterns and history are personal data. However, when this data is detailed enough to reveal an individual's daily routine, it becomes sensitive as it could be misused for stalking or other privacy invasions.

# Metropolis Asset Inventory

## 

## Figure2: Simplified Example on the Data Assets

[](Asset_Inventoryy.xlsx)

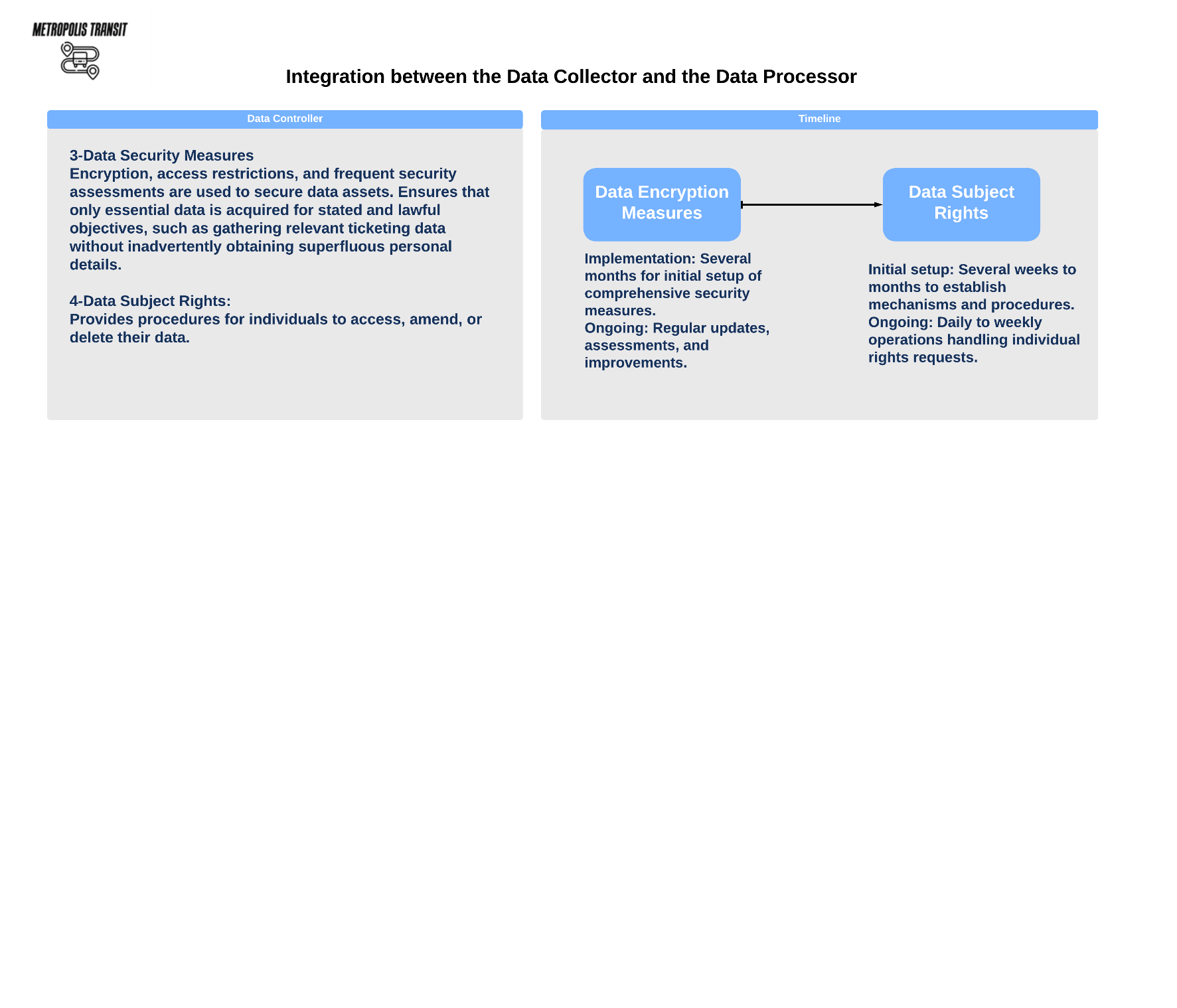
[Asset Inventory.jpeg](Asset%20Inventory.jpeg)

## Figure3: Simplified Network Diagram that represent the Metropolis Subnets

# What is the role for the Data Controller and the Data processor within the domain of Metropolis

In the context of Metropolis Transit, these roles are particularly critical due to the sensitivity and variety of data being handled. The Data Controller in Metropolis Transit, would set policies and direct how all the different data assets are handled, ensuring compliance with legal requirements and ethical standards. The Data Processor would handle the actual processing of data, such as managing CCTV footage, analyzing ticketing data, or maintaining employee databases, all under the guidance and instructions of Metropolis Transit data controller and processor. Both roles are bound by the need to protect the privacy and security of individuals' data and ensure that the operations of Metropolis Transit are efficient, lawful, and respectful of data subjects' rights.

## Data Collector Responsibilities:



## Data Processor Responsibilities:

# Risk Assessment

The provided link contains risk assessment for Metropolis infrastructure adding to that Assessing the Vulnerabilities, Threats, and the impact of each on the Data assets and other types of assets that are in metropolis.

[Risk Management.xlsx](Risk%20Management.xlsx)

# Data Subject Rights

## Right To Access:

The right to access allows individuals to know what personal data Metropolis Transit holds about them, how it's being used, and whom it's shared with. It's crucial for transparency and enables individuals to verify the accuracy of their data

Procedure: [Right To Access.docx](Right%20To%20Access.docx)

## Right To Rectification:

refers to the entitlement of individuals (data subjects) to have inaccurate or incomplete personal data corrected or completed

procedure: [Right To Rectification.docx](Right%20To%20Rectification.docx)

## Right To be Forgotten:

allows individuals to request the deletion or removal of personal data that is held by an organization when there is no compelling reason for its continued processing

procedure: [Right To be Forgotten.docx](Right%20To%20be%20Forgotten.docx)

## Right To Data Portability:

Metropolis will be able to transfer the personal data directly to another data controller specified by the individual

Procedure: [Right To Data Portability.docx](Right%20To%20Data%20Portability.docx)