LOGIC INSIGHTS

# Data Governance: *Beyond Data Management*

*Like Any Asset, Data Requires Care and Maintenance!*

Data governance has risen to the forefront of many companies across different industries. Still, most of them mainly adopt data governance measures due to increased government regulations regarding the collection and handling of data, along with the huge reputational risk from data breaches or other types of incidents. However, data governance isn't just about compliance or security, as both often create a disconnect between governance and business impact. Companies need to go beyond meeting baseline regulatory and security standards in order to translate data investments into value in their core business. Without quality-assuring governance, companies not only miss out on data-driven opportunities; they waste resources. It was reported that an average of 30% of employees' time was spent on non-value-added tasks because of poor data quality and availability (1). Data governance is about having a common and shared understanding of data, and efficiently managing it in order to optimize business value. In practice, it's a combination of

A - POLICIES, B- PEOPLE AND ORGANIZATION, C- TECHNOLOGY

## *WHY IS DATA PRIVACY IMPORTANT?* (2)

**Competitive Advantage**

Organisations are finding efficient and economical ways to run their businesses which involve transferring data outside of their jurisdictions and are using data analutics to create new revenue steams.

**Consumer Trust**

Organisations need new mechanisms to build consumer trust and confidence as they address emerging challenges in business, risk management, and compliance.

**Interconnected World**

Traditional ways of doing business are no longer valid in an increasingly interconnected world, with people and information being spread across multiple countries.

**Privacy Regulation**

Regulatory bodies are taking an increasingly tough stance on privacy, imposing heavy fines on breaches for violations of individulas right to privacy.

(1) Designing data governance that delivers value, McKinsey, 2020
(2) Data privacy in Egypt: what you need to know, PwC

# *SO HOW CAN COMPANIES IMPLEMENT DATA GOVERNANCE THAT IS VALUABLE, SUSTAINABLE, AND SCALABLE?*

1.

## Develop A Well-defined Data Governance Framework:

This starts with assessing current data-related challenges, identifying gaps in data utilization and prioritizing key focus areas, all of which need to be covered as part of data governance initiative. Companies should shortlist the best-suited data governance framework that covers all the key areas in scope, such as data privacy, data access, metadata management. A data governance framework directs how data will be managed and controlled while complying with external standards set by industry associations, government agencies, and other stakeholders. Among the areas commonly included in data governance frameworks are data policies, such as data availability, data integrity, data quality, data security, and data usability.

## 4 Aspects to Consider When Building Your Data Governance Framework:

### DISTINCT USE CASES

It is essential to connect data governance to business results by considering revenue, cost and risk.

### QUANTIFIABLE VALUE

The impact of the data governance implementation needs to be measurable.

### BUILDING DATA CAPABILITIES

Data governance framework should outline the capabilities that are needed to improve the value of data for users and address individual needs for data usage.

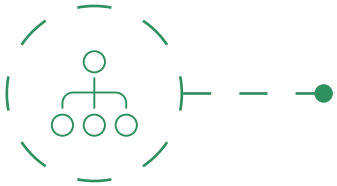
### SCALABLE DELIVERY MODEL

A data governance program must have a scalable delivery model (one that is flexible and where the addition of new resources brings increasing returns). This way, organizations can address more use cases, impact more teams and tools, bring more with less effort.

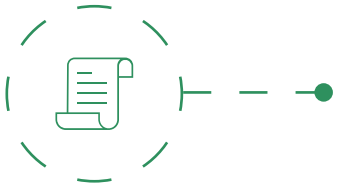
2.

## Ensure Compliance with Law

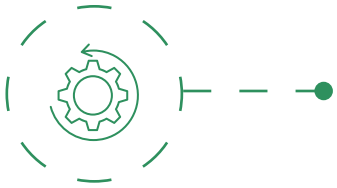
On July 2020, Egypt's Government issued the Data Protection Law, which establishes various standards and controls governing the processing and handling of personal data. The Law imposes a licensing, permit and security accreditation framework for data processing, data control, dealing in sensitive data, electronic marketing, and cross-border transfer of data. It also implies the following:



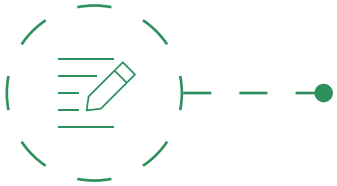
**Any organization that controls or processes personal data must appoint a data protection officer ("DPO"), who is an Egyptian resident. DPO is responsible for monitoring the organization's compliance with the law, conducting regular inspections and taking corrective actions to remove personal data breaches.**



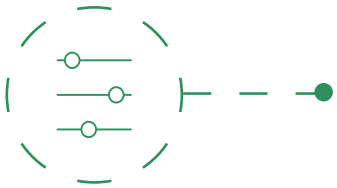
**The law solely applies to personal data that has been electronically processed, whether partially or entirely, hence data held exclusively in a physical format is not regulated.**



**A controller or a processor outside Egypt is required to appoint a local representative in Egypt, as a point of contact for Egyptian data subjects.**



**Organizations are required to keep a record of their processing activities (the type of data processed, the purposes for which it is used, the duration of the processing activities, its scope and limits, the mechanism of its update or deletion, and a description of the technical and organizational security measures.**



**Organizations should review technical controls they have in place, to ascertain whether they are fit for purpose and support data protection requirements.**

The Data Protection Law puts a general accountability obligation under which organizations must be able to demonstrate their compliance with the Law. Egyptian companies will have a lot of work to do and will have to implement a wide range of measures to comply with the law as the law imposes heavy fees and penalties for non-compliance. The road might be easier for multinational organizations that already abide by the GDPR, or similar privacy frameworks, as the Law doesn't present many new concepts.

# 3.

## Define Clear Accountabilities

Successful data governance requires multilayer management that is focused on business but spans both business and IT. Various departments use data for different purposes, making it critical to appoint data governance advocates from diverging lines of business. So, what should your data governance organizational structure look like? What are the teams' roles at the tactical, operational, and strategic level? Figure (1) illustrates what a typical data governance team structure includes:

4.

## Manage Data Quality Over Data Lifecycle

The value of data is greater if its quality is assessed and maintained throughout a well-understood data-lifecycle; data creation, storage, usage, archival and deletion. Each phase has distinct governance needs and is regulated by a set of policies that maximizes the data's value. Data life cycle management (DLM) process places value on data at each stage of its lifecycle. Once data is no longer useful, organizations can leverage a range of solutions to reduce costs such as data backup, replication, and archiving. For example, it can be moved to less-costly storage located on-premises, in the cloud, or in network attached storage.

The quality level must be defined in the policy framework and upheld by the tools and technology. A consistent approach to data-quality in the context of lifecycle helps the business to identify weakness points where data-quality suffers. Consistent and well-understood quality assessments allow stakeholders to quickly establish what level of trust to apply and ideally allows them to make modifications to processes that denigrate data-quality.

**For example, with Uber facilitating 14 million trips per day, how can they ensure that their decisions are backed up by high quality data? And How to ensure the quality of data sources? Recently, Uber launched its Data quality monitor (DQM), a solution that leverages statistical modeling to manage the quality of data sources across Uber's infrastructure. DQM relies on statistical modeling to detect the most destructive anomalies in data sources and alert the relevant parties, but without flagging so many errors that owners become overwhelmed.**

5.

## Manage Data Access

Many organizations have minimal access management systems in place. According to Ponemon Institute, 71% of end users said they often had access to data they should not see and 80% of IT personnel believed their firms did not have a data model that enforces strict data access privileges. Employees with needlessly excessive data access privileges represent a growing risk for organizations due to both accidental and conscious exposure of sensitive or critical data. Therefore, it's critical to have practical policies and tools in place to facilitate access to authorized stakeholders while maintaining appropriate security. You need to identify who needs what data & when.

When deciding what data people need to access, consider both what they will need to do with the data and what level of access they need to do their jobs. For example, a salesperson will need access to his customer database but will not have access to the company's full customer database or company's accounts payable. Assigning role-based access control (RBAC) helps you protect resources by managing who has access to resources, what they can do with those resources, and what resources they can access. Also, you need to set up recurring monitoring and reporting to check what people are doing with the access they have.

## *DATA GOVERNANCE MATURITY MODEL - IBM*

Companies' maturity level could differ greatly; some may be completely unaware of any data governance activities with no ownership, security, or any system defined for data in the organization, others may be highly mature where data governance becomes an enterprise-wide effort that provides the company with a competitive edge in the market.
One way of measuring the effectiveness of your data governance program is to assess it against an existing maturity model. Data governance maturity refers to the level of data management process and optimization you have built into your business. This can help by indicating; Where are you with the data governance program? How are you progressing? What are some of the steps you need to take in order to evolve your program? There's no one-size-fits-all model for data maturity, and even when you do select one, you'll need to adapt it to suit your organization:

### LEVEL 1: INITIAL

There is little to no awareness of the importance of data and there are no set standards for managing data.

### LEVEL 2: MANAGED

The importance of data in the organization is realized.

### LEVEL 3: DEFINED

Data regulation and management guidelines are defined better and are integrated with the company processes.

### LEVEL 4: QUANTITATIVELY MANAGED

Measurable quality goals are set for each project, data process and maintenance.

### LEVEL 5: OPTIMIZING

Data governance becomes an enterprise-wide effort that improves productivity and efficiency.

# 6.

## Measure and Sustain

Data Governance is not just an initiative you carry out at a given time. It is a continuous program that you need to embed within the fabric of your organization. Data governance metrics provide an opportunity to establish a baseline to "know what bad data means, and potentially, what good data could mean, and thus create a starting point to get the broader organization to understand the need for better data. Metrics can also help get the organization aligned on the expectations of the governance program, along with engaging different stakeholders. To achieve this, the organization must:

Define clear KPI's and baselines that are aligned with program objectives.

Evaluate on regular basis, via different audits (compliance, security, quality, etc.), how much the program is on track with regards to these baselines.

Make the necessary adjustments when required.

## *WHAT DOES POOR DATA GOVERNANCE LEAD TO?*

What risks can the organization face? Organizations that fail to protect personal data and comply with data privacy regulations aren't just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and most importantly permanant loss of consumer trust (3).

### REGULATORY

Regulators may require the provision of information, conduct audits, and obtain access to premises if they determine it is necessary.

### REPUTATIONAL

Non-compliance with the law could result in brand damage, loss of consumer trust, loss of employee trust and consumemr attrition.

### FINANCIAL AND CRIMINAL

Fines and, in some countries potential prison sentences, could be enforced depending on the violation. You may also experience loss of revenue and high litigation and remediation costs.

### OPERATIONAL

Data subjects can impose data processing bans and order the correction of an infringement. This could result in restricted operations and invalidated data transfers.

(3) Data privacy in Egypt: what you need to know, PwC