protiviti®

Global Business Consulting

Navigating Data Privacy in the Middle East

Balancing Business Needs with Data Privacy

Face the Future with Confidence®

Index

Executive Summary

Data has become a crucial driver for businesses in today's digital age, as organizations can leverage data from various sources, including consumer behavior and operational insights, to make informed decisions, improve efficiency, and drive innovation. However, consumers are increasingly concerned about how businesses handle their personal data, and the rise of data breaches has eroded consumer trust in how businesses handle their personal information. Considering the trends consumers are expected to make buying decisions based on a company's data protection practices. Therefore, privacy has become a crucial agenda for organizations, as proper handling of personal information is essential for building consumer trust and experience.

Regulatory bodies worldwide have recognized this trend, as evidenced by the introduction of multiple privacy regulations. In the GCC, there has been increased awareness from consumers, increased focus from organizations, and the introduction of new regulations to strengthen the data privacy regime. Protiviti conducted a survey of over 100 organizations across various industries, including BFSI, Telecom, IT/ITES, and government institutions, to understand the current state of data privacy programs, key areas of focus, and expected roadmaps for the future. This whitepaper aims to provide an independent study of the survey results and offer perspectives and considerations for GCC organizations embarking on the data privacy journey.

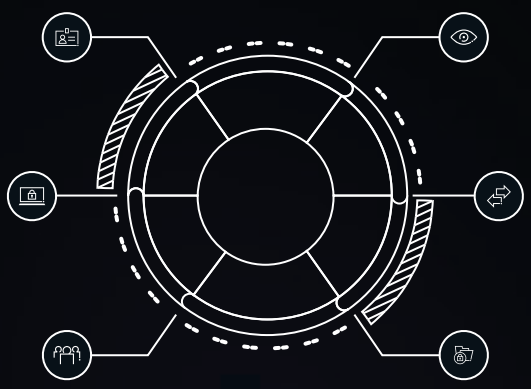
Key Insights

Driving Force

56% highlighted regulatory requirements as primary drivers for Data Privacy Programs

Governance

47% highlighted Data Privacy Programs are not periodically monitored or reported due to lack of Governance



Biggest Challenge

76% highlighted reduced visibility as the most significant challenge

Budget

43% are yet to allocate a budget for Privacy Program

Privacy Program

Only 21% have operationalized a Data Privacy Program

Cloud

67% have concerns on Cloud Service Providers providing clear visibility on personal data

Key takeaways of this report:

- In addition to understanding local data privacy regulations, organizations should equally consider elements of increasing customer trust as part of their Data Privacy Program.
- Privacy responsibility and ownership seems to be scattered across the organization (only 27% having dedicated Data Privacy Departments and 40% confirming Data Privacy is with Information Security Department), it is critical for senior leadership to define appropriate privacy driven roles and responsibilities and Governance structure
- Based on the regulations and the adherence to respective timelines, privacy executives in the organization must prioritize budget allocation for implementation of Data Privacy Program within the organization
- Strategizing the roadmap for data privacy implementation will help organizations in enhancing consumer trust along with achieving compliance with local regulations
- With 40% of organizations confirming their intention to acquire technologies for addressing privacy requests and Data Subject Access Requests, automation will be essential for organizations to ensure seamless fulfillment of privacy requirements.

Introduction

Data Privacy encompasses the rights of individuals to control the collection, use, and disclosure of personally identifiable information or personal information[1]

The Pressing Importance of Data Privacy:

Data Privacy today has become a fundamental human right that aims to preserve an individual's privacy, dignity, and autonomy by giving them control and visibility over how their data is collected, processed, and disclosed by businesses. Data and Technology are codependent today and both are critical for enabling business operations and driving transformations. As an outcome of this codependence, massive data is produced which is increasingly becoming complex to manage and protect. This is especially relevant in the GCC where digital transformation and innovation are driving forces fueling economic growth. A fundamental part of this digital transformation comes with the adoption of the Cloud, Internet of Things (IoT) devices, Application Programming Interface (APIs), and All things Smart (smart homes, voice assistants etc) which is generating an incredible amount of data on a daily basis.

Further, the adoption rate of such technologies catapulted amongst customers over the last decade, but they are also becoming more and more conscious about how their personal data is being used by businesses[2] since misuse is rampant. Governments are also recognizing the need to uphold privacy. The evidence can be seen through the various regulations introduced across the globe as well as in the GCC to effectively regulate the processing of personal data and uphold the privacy rights of its residents and citizens.

1 Personal Information is information that relates to an identified or identifiable natural person example name, mobile number, passport no etc

2 https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=47de3bd8487e

How is Privacy different from Data Security?

Data privacy and data security are two dependent yet distinguished concepts in the area of data protection. Data privacy refers to the protection of personal information from unauthorized access, use, or disclosure. It focuses primarily on ensuring that individuals have control over their personal data and that it is handled in a way that respects their privacy rights (defined by Law or Regulation, varied by meaning in countries). Data privacy is concerned with preventing the misuse of data, such as identity theft, sale of data, unauthorized profiling, or discrimination based on personal data.

Data security, on the other hand, refers to the protection of data from unauthorized access, alteration, destruction, or theft. It involves putting in place technical and organizational measures to safeguard critical data from a range of threats, such as cyberattacks, malware, or physical theft. Data security is concerned with protecting data as an asset in its entirety and doesn't limit to the protection of personal information. Data security is a core enabler for data privacy. However, the scope of data privacy extends beyond data security as it addresses other areas, such as data subject rights, choice and consent, cross-border transfers, privacy by design and many more.

"Digital Transformation has brought forth tremendous benefits, however, organizations must balance the criticality of business optimization with data security and privacy requirements that should be integrated by default"

– Siva S, Managing Director

Current Drivers for Data Privacy in the GCC

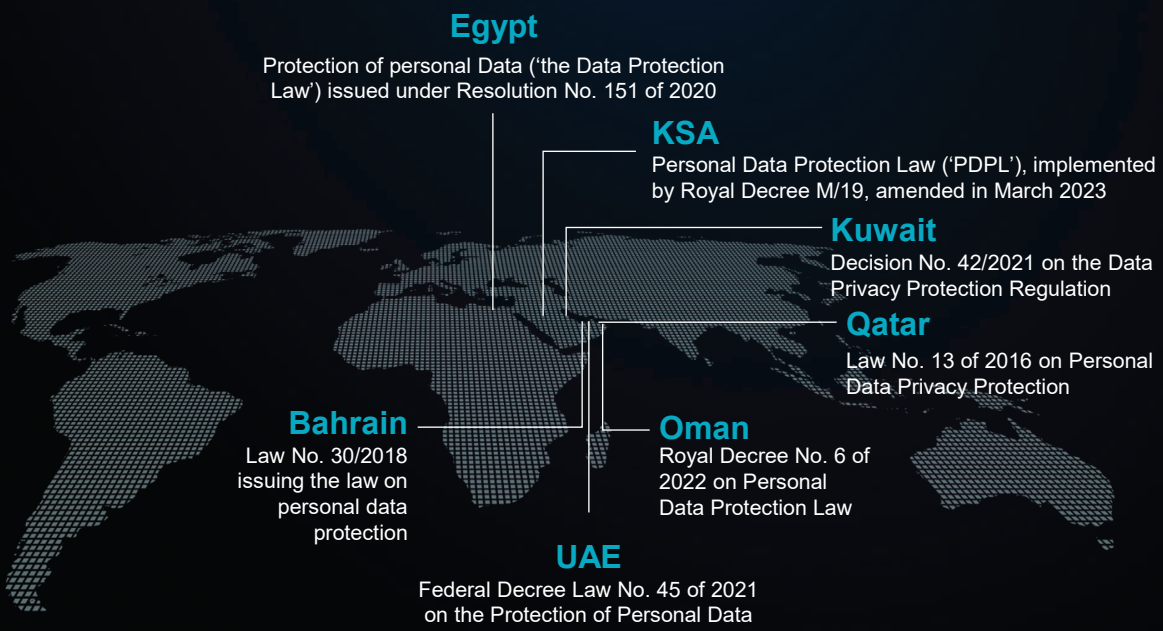
GCC region is witnessing an increasing adoption of privacy programs. The top 3 business drivers for adoption of the privacy programs are:

Regulatory Landscape:

By the end of 2024, Gartner predicts that 75% of the world's population will have its personal data covered under modern privacy regulations[3] . Studying the data privacy trends over the last decade, regulations have been the primary evangelist for Data Privacy. With the advent of the General Data Protection Regulations (GDPR) in 2016, we have witnessed multiple countries across the globe establish new/ revised data protection and privacy regulations. These regulations are also followed through with the imposition of fines and penalties on industry giants which clearly outlines the repercussions of not adopting the regulations appropriately. Regulators in the GCC have made significant strides on this subject and introduced multiple regulations around data protection and privacy. A few notable updates include:

56%

identified regulatory obligations as key driver for their Data Privacy Program



3 https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024

Consumer Trust

According to a survey conducted by 'Consumers International', Consumers in the MENA are one of the most worried populations in the world with regards to how their data is collected and kept private online[4].

In another global survey conducted by Cisco in 2022[5], 79% of the survey respondents stated that they do not have visibility on how companies process their personal data. Further, in the same survey, 90% of the respondents would not buy from organizations if they did not adequately protect their data. Consumer behavior has changed over time to not inherently trust organizations with their data. This behavior shift is enabling businesses to be more transparent with their consumers with the primary goal of winning their trust. The section below summarizes a few key expectations concerning data privacy by the consumer from organizations.

> "Building consumer trust is a primary driving factor for businesses when building privacy and transparency for their consumer base"

Key Consumer Expectations

Respect digital privacy
Avoid unnecessary profiling of my data to wrongly influence buying decisions

Greater visibility
Clarify how my personal data is processed

Protect Data
Ensure my personal data is protected from unauthorized access

Ease of access
Organizations should be easy to reach and enable ease of access to my data

Respect preferences
Personalize my customer journey and respect my choices

Better control
Ability to decide how my personal data can be utilized

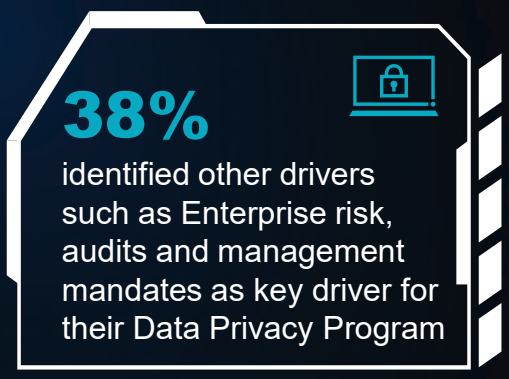
4 https://www.consumersinternational.org/media/314598/privacy-mena-briefing-dec2019.pdf
5 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

Contractual Obligations

Contractual obligations serve as a crucial driver for data privacy, particularly in the context of business transactions and relationships. Organizations often enter into agreements or contracts that outline the terms and conditions of data handling, processing, and protection. By explicitly defining the responsibilities and expectations of all parties involved, contractual obligations create accountability and foster a culture of privacy within business operations.

Contracts commonly include provisions related to data security measures, data breach notification, data sharing limitations, and the handling of sensitive information. These obligations help protect individuals' personal data from unauthorized access, disclosure, or misuse.

Organizations in the GCC region work with multiple third parties as is the norm of the global economy today. These third parties range from Cloud Service Providers to Outsourced / Freelanced Developers to Managed Services Providers. Contractual obligations thus play a critical role in safeguarding data privacy by setting clear expectations, establishing legal protections, and fostering trust between parties involved in data processing activities.



Data Privacy Program: Top Inhibitors and Focus Areas

The increasing scrutiny around data privacy in GCC, along with the rising amount of personal data being collected and processed, the risks associated with data privacy breaches have significantly grown. The growing concerns around data privacy and the evolving regulatory landscape have amplified the need for understanding key concerns that impact data privacy programs. While regulations and consumer trust are key drivers for data privacy, the trifecta is incomplete without evaluating the benefit to businesses. We conducted a survey to understand the organizational view on the data privacy program and the typical challenges for establishing a data privacy program.

Top 5 Data Privacy Challenges

- Visibility over Personal Data
- Data Retention and Disposal
- Security Incidents and Data Breaches
- Localization and Cross Border Transfer
- Consent Management

Visibility over Personal Data

76%

Identified Data Visibility as their biggest challenge for Data Privacy Program

Visibility over personal data refers to the organization's ability to track and monitor the personal data it collects, processes, and stores. Without a clear understanding of where personal data resides, organizations may not be able to adequately protect it or respond to data breaches in a timely and effective manner. To combat this challenge, businesses should undertake a **data discovery** exercise to identify and map out the collection, storage, processing, and transfer of personal data within their environment.

"Visibility over Personal Data, Data Retention / Disposal and Identifying / Responding to data breaches are the top Challenges that organizations across the Middle East are facing today"

Data Retention and Disposal

Data retention refers to the period for which organizations keep personal data. This is decided based on the applicable regulations and business needs. Data disposal, however, refers to the process of securely deleting or destroying personal data once it is no longer necessary to retain it. Data disposal methods include physical destruction of electronic storage media and secure deletion from electronic devices.

Businesses recognize the complexities involved in data retention and disposal, considering that all data processed in most organizations are retained indefinitely and is spread across structured/unstructured data storage mechanisms. Poor data governance mechanisms, ineffective data minimization practices, and absence of effective data disposal mechanisms may further cascade the complexities. Businesses should establish a formalized program (employing robust data governance practices) to identify the categories of data handled. Businesses should clearly define the retention policy and schedules, and implement data disposal practices that ensure personal data is not used/ retained beyond the lawful purposes.

Security Incidents and Data Breaches

Security incidents or data breaches occur when there is a violation of confidentiality, integrity, or availability of an organization's data (including personal data). These incidents can have severe consequences for organizations, as personal data is often one of their most valuable assets, and it is essential to protect it. As per IBM Cost of Data Breach study[6], the Middle East region was noted as the 2nd highest average total cost of data breaches. Further, average time taken by organizations globally to identify and contain a data breach was 277 days. This highlights pressing questions for businesses to ask, "Do I have the right people, process, technologies, and supply chain to effectively identify and manage security incidents and data breaches?", "how do I determine whether a security incident is a potential data breach?"

Organizations should relook at their security monitoring and incident management program to ensure early identification of potential breaches. Further, the security incident management processes should be integrated to effectively identify privacy incidents, and procedures should be defined to manage breach notification requirements.

"Organizations need to perform data discovery on structured and unstructured data through top down and bottom-up approach to perform data discovery activities"

6 Cost of a Data Breach Report 2022 by Ponemon Institute sponsored by IBM

Localization and Cross-border Transfers

Data localization and cross-border transfer restrictions refer to the requirement for organizations to store personal data within a specific country or region and the limitations placed on transferring personal data outside that country or region. On one hand, these restrictions are intended to ensure individuals can effectively exercise their legal rights over their personal information. On the other hand, it may increase complexity in operations, increase service costs and limit use of digital capabilities outside region boundaries.

To strike a balance, organizations must understand the applicable legal and regulatory requirements of each of their operational locations and take steps to mitigate data privacy risks associated with transferring personal data across borders. Suitable technical measures and legal instruments should be considered to ensure lawful cross-border data transfers.

50% identified data localization/ cross-border transfers as **Top 5** major concern for privacy compliance

54% of organizations limit personal processing within the region, while **35%** rely on adequacy measures, use of data protection agreements or are working with specialists to appropriate design strategies

Consent Management

Consent management refers to a system, process, or set of policies that is used by an organization to inform users about how their personal data will be used and collected and give them control over what personal data they are willing to share. Multiple regulations in the GCC recognize 'Consent' as one of the key lawful basis for processing personal information and set key standards for its application and compliance.

Use of blanket consent or relying on consent as the only basis for processing may violate the provisions of current privacy legislation considering that individuals have the right to withdraw consent.
Businesses should relook at their consent collection and management practices to ensure consent obtained from Personal Data Owner is informed, specific, and unambiguous. Also, businesses are required to maintain records to prove consent was obtained and enable accessible mechanisms for consent withdrawal.

Third-party Risk Management

Organizations consistently engage third-party service providers to support their business processes. However, the use of third-party vendors is considered one of the top enterprise-level risks impacting the organization. Further, recent breaches prove that the traditional approach towards vendor onboarding and management needs significant updates.

Businesses should consider additional measures prior to sharing personal data with third-party vendors ("Data Processors").Conducting data privacy / security due diligence prior to hiring third parties, incorporating contractual obligations around data privacy/ security, and regularly monitoring compliance are few essential considerations

52% of organizations are still addressing third-party risks using NDA's and Confidentiality Agreements

Only **29%** of organizations are planning investments to strengthen their third-party risk management

"With an increased reliance on data managed by third parties, organizations must prioritize assessing the security and privacy maturity of their supply chain"

Data Subject Access Requests

33% highlighted concerns in implementing process to manage Data Subject Rights

40% of organizations are planning to leverage technologies and automation capabilities to address challenges concerning Data Subject access requests

Data Subject rights are designed to enable individuals to take control of their personal data and ensure its lawful and fair processing by organizations. As an example, this would mean that individuals can request companies for a copy of all personal data or request for correction/deletion of certain personal data, and subject to certain exemptions, businesses are expected to fulfil the requests within a time frame (for example 30 days in the case of Saudi Arabia).

Data Subject access requests can be daunting for businesses to address as it requires a comprehensive visibility over the personal data, effective data management practices to streamline workflows and ensure timely fulfilment. To address these requirements, organizations need to enforce better control over personal data, establish standard operating procedures and leverage technical solutions to manage the lifecycle of such requests received from Individuals to ensure timely fulfilment of Data Subject requests.

"A central component of any data protection law is upholding the rights of individuals i.e. data subjects. Organizations must process requests from data subjects timely and in accordance with the law. This requires the cooperation of multiple departments within your organization."

Data Privacy Program Governance

Privacy Ownership and Oversight

Ensuring that Data Privacy Program continues to be appropriately governed and respective oversight is maintained, contributes significantly to the success of the program. To understand where does Privacy currently belong in organizations, we asked “Who is responsible for governing and managing data privacy programs and initiatives in your organization?”

27%

Highlighted that a dedicated Data privacy department has been formed to govern the Data Privacy program

40%

Highlighted that information security department already governs the data privacy program

12%

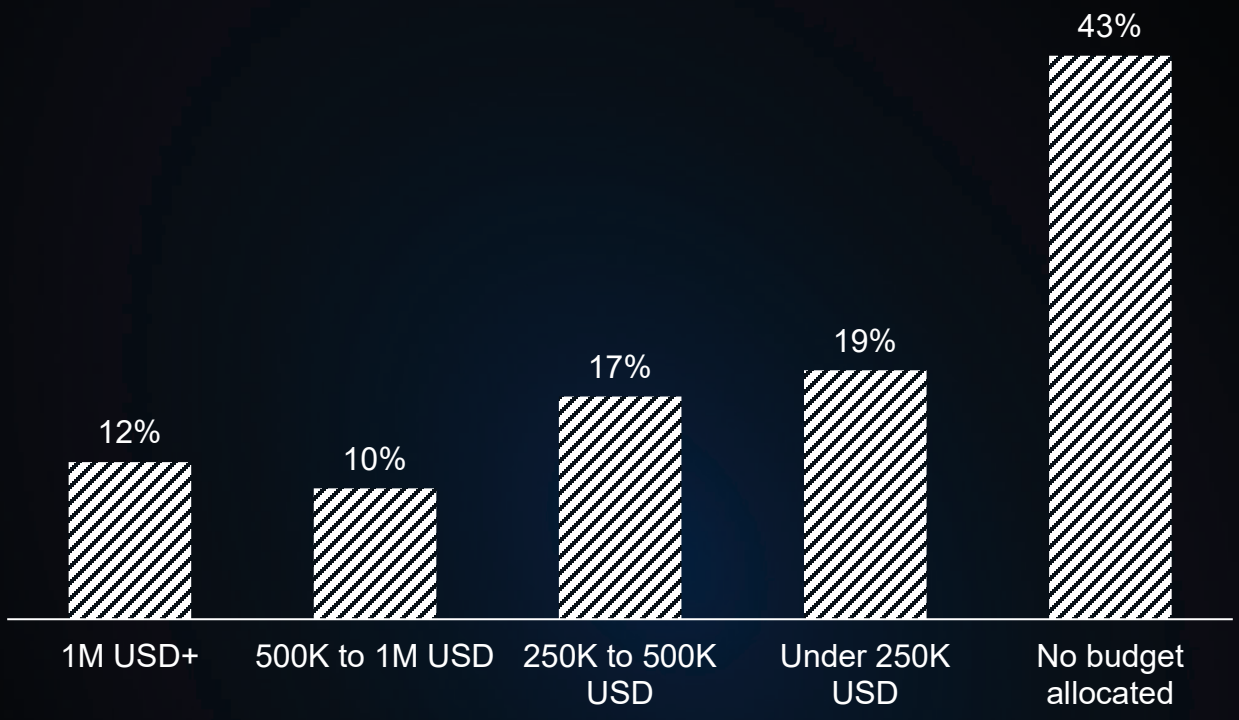
Highlighted that legal or Risk Mngt currently governs the data privacy program

47%

Highlighted that data privacy program is not monitored or reported to Senior Management periodically

While the spectrum of drivers exists, the need to establish a formalized program is very clear and requires dedicated focus. Having a privacy policy published on a website just does not cut it anymore. Businesses should consider that Data Privacy, like Information Security, requires effective governance to adequately embed privacy within their business processes and service offerings. Further, considering that the motive of a data privacy program is not just to ensure compliance but also to uphold the individual’s privacy rights, adequate independence and Senior Management oversight are essential to establish a robust program.

Investment and Budget



While 57% of the respondents highlighted that a dedicated budget was allocated,12% stated around 1M+ USD has been allocated.

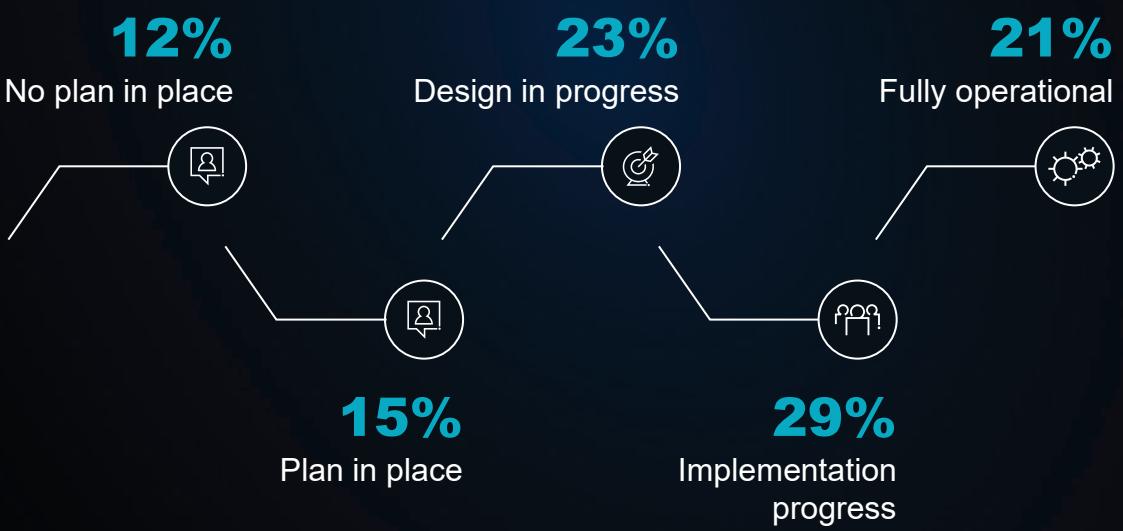
However, 43% of organizations have not yet allocated a budget for privacy program. This highlights that organizations in the GCC need to emphasize on prioritizing budget allocation for their privacy program.

We estimate that budget allocation for Data Privacy will significantly improve over the next few years, considering the growing appetite for automation.

Building a Resilient Data Privacy Program in a Connected World

The journey from designing to operationalizing a Data Privacy program will be a challenge for many organizations and being proactive will serve an edge for the businesses with their consumers. A typical compliance journey involves many considerations including regulatory and litigation risks for non-compliance. Proactive businesses are assessing their current capabilities, designing their future state, and operationalizing ongoing programs to allow for sustainable and demonstrable compliance.

The section below illustrates the current maturity of privacy programs in the GCC. It is interesting to note that only 21% responded that their data privacy program is fully operational and is in continual improvement.



Keeping in mind the various complexities and legalities involved, it is important to have a structured approach to data privacy. Given our experience working with clients across the globe and especially in the GCC, a generic approach to privacy does not work, businesses should consider their strategy, business context, current state, existing capabilities, and risk appetites while implementing the Data Privacy program. The further section explores a scalable approach that could be considered by businesses embarking on their Data Privacy journey.

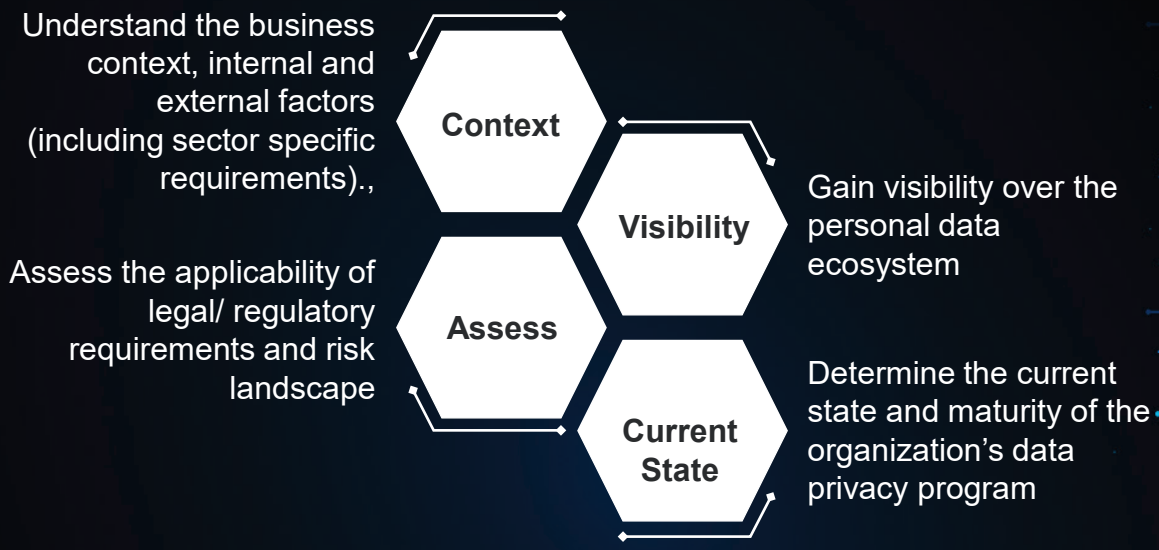
Typical Journey for a Data Privacy Program

The privacy program and suggested approach can be structured into 4 key components – "Visualize", "Strategize", "Operationalize" and "Realize". Sections in subsequent pages further elaborate key aspects to be considered under each program component.

"A Successful Data Privacy Program demands organizations to move from SILOS to SYNERGY in bringing together Businesses, Information Technology and Security teams together for one collaborative goal"

Visualize

Organizations should plan their data privacy journey by following a structured approach that considers aspects such as personal data ecosystem, applicable legal/ regulatory requirements and risk landscape. In this stage it is important to contextualize the data privacy program, considering the internal and external factors, to understand the current state prior to establishing the program strategy.



Strategize

The purpose of a Data Privacy Program is to ensure that personal data is managed in a way that complies with applicable privacy laws and regulations, respects the privacy rights of individuals, and maintains the trust of stakeholders. In this stage it is key to strategize and create a foolproof design that considers the business context, risk landscape and envisioned target state.

There are three primary objectives that are most often considered for a Data Privacy Program:

a) Ensuring legal, regulatory and contractual compliance
b) Upholding privacy rights of Individuals
c) Enhancing customer trust

Section below illustrates the key activities that should be considered in this stage:

SWOT ANALYSIS	STRATEGIC INTENT	GAIN COMMITMENT	FRAMEWORK	STRATEGIC ROAD MAP
Conduct a SWOT analysis to determine the areas that need to be leveraged, optimized, strengthened and managed.	Define strategic intent including program vision, mission, goals, and objectives, that the organization intends to achieve.	Gain management commitment towards the implementation of the privacy program.	Develop a comprehensive framework to lay out the expected methodologies and process.	Design a strategic road map considering the intent and envisioned target state

Operationalize

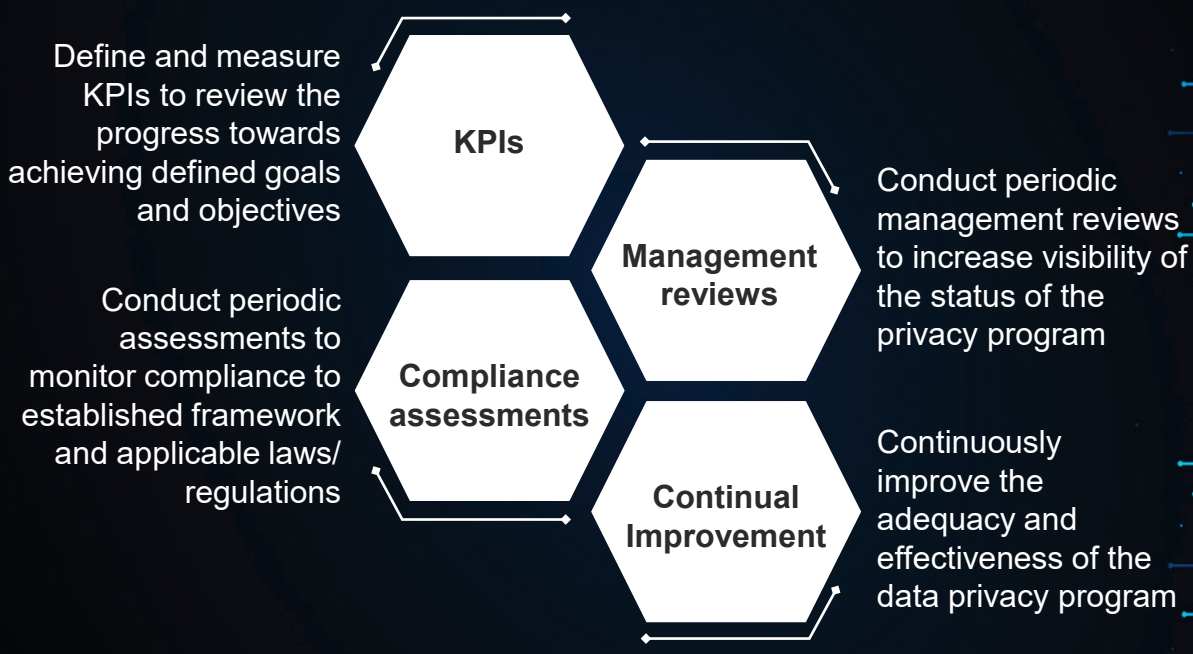
Translating design into operations is a crucial endeavor and requires effective planning, coordination, and targeted efforts. Operationalization in any organization is a 'Change Management' driver and should start with the organization's internal culture. The section below summarizes key activities that should be considered in this stage:

PEOPLE	PROCESS	TECHNOLOGY	SUPPLY CHAIN
• Establish program oversight • Establish Target Operating Model • Embed privacy culture through training and awareness	• Operationalize framework • Embed PbD (Privacy by Design) principles into Business Ops • Address data retention and disposal	• Privacy-enhancing technologies • Embed PbD principles into the technology lifecycle	• Managing supply chain risks • Partnership with privacy advisors, legal counsel and technology vendors.

Realize

The most important phase of any program is to ensure that the program is achieving the envisioned goals, objectives and can sustain the evolving business landscape. This is where periodic monitoring becomes a key yardstick to assess the program's health and to ascertain if the intended objectives are met.

Key monitoring mechanisms that should be considered are illustrated in the figure.



The program can be further realized and complemented through independent certifications and automation capabilities to sustain a mature program.

Interestingly, 35% of the survey respondents are planning to adopt certifications such as ISO 27701 alongside ISO 27001 which will assist in improving the maturity of their Data Privacy Programs.

Data Privacy and the evolving Technology Landscape

The technology landscape is massively evolving for businesses across the GCC as organizations consistently explore avenues to utilize cutting edge technologies to solve business problems. With the adoption of certain technologies, careful strategizing is critical to ensure that privacy considerations defined can remain baselined across the technology landscape. Some of the instances of strategic considerations for ensuring privacy in an evolving technology landscape are:

CLOUD

Cloud has brought forth tremendous opportunities to businesses in lowering costs while upscaling compute capabilities across the world. With the increased adoption of the cloud in the regions, it is critical for organizations to thoroughly assess their privacy needs prior to migrating to cloud or adopting cloud services

Privacy controls in cloud: 67% of organizations highlighted concerns on visibility on personal data access by Cloud Service Provider (CSP). In order to cater to this challenge, assessing the sensitivity and critically of the data being migrating to cloud will assist in categorizing privacy and regulatory requirements.

Secure configuration: 50% of organizations are deeply concerned about misconfigurations issues. Define, implement and monitor data security/ privacy configurations/ best practices on the adopted cloud service model and periodically ensure configurations are appropriately defined.

Trusted CSP: Comprehensive evaluate the Cloud Service Providers on their Security measures, certifications and tools offered by the provider that can cater to defined privacy controls.

Compliance: Ensuring the CSP caters to local and regulatory requirements (such as Data localization) helps balance this concern. However, only 52% organizations plan to periodically govern the cloud service provider for compliance and vulnerability management practices.

Awareness: Educate your end users and stakeholders on privacy practices in the cloud environment.

"Cloud offers incredible scalability, however, to confidently manage, secure operations, organizations must diligently assess and mitigate risks, prioritize relevant security measures, and remain vigilant in monitoring and compliance."

INTERNET OF THINGS (IoT)

IoT devices often gather sensitive data about individuals, such as their location, habits, health, and preferences. Due to lower security and privacy measures built in, personal data can be vulnerable to unauthorized access, misuse or exploitation.

- **User consent and transparency**: Providing clear and understandable privacy notices to users, outlining what data is collected, how it is used, and with whom it is shared will help improve customer transparency. Where possible, provide consumers with granular control over their data and manage consent accordingly.

- **Data minimization and purpose limitation**: Collect only the minimum amount of data necessary for data retention. Controls for data limitation and collection should be designed carefully and accordingly implemented.

- **Strong authentication and access controls**: Often IoT devices have weak authentication mechanisms. It is critical to ensure that devices support strong authentication mechanisms, such as unique identifiers or passwords. Further, access should be restricted, minimum baseline security controls must be identified, implemented and monitored periodically to ensure continued compliance.

- **Secure data transmission**: Implement secure protocols and encryption mechanisms to ensure that data transmitted by IoT devices is protected from interception or unauthorized access. This includes using secure communication channels, such as Transport Layer Security (TLS), and encrypting sensitive data during transmission.

CONSUMER IDENTITY AND ACCESS MANAGEMENT (CIAM)

CIAM solutions are fast becoming a necessity to enhance the consumer experience and elevate security for consumers. Ensuring that sensitive data such as names, addresses, and financial details are securely stored and accessed only by authorized individuals is the key.

- **Granular Access Controls**: Employ granular access controls to limit data access based on their roles and permissions. This ensures that consumers' personal information is only accessible to authorized individuals within the organization.

- **Consent Management:** Implement a comprehensive consent management system (CIAM should have consent management) that allows consumers to provide informed consent for data collection, processing, and sharing. Provide clear and transparent options for consumers to manage their privacy preferences and easily withdraw consent if desired.

- **Regular Auditing and Monitoring**: Regularly audit and monitor the CIAM solution to detect any unauthorized access attempts, suspicious activities, or breaches. Implement logging and monitoring tools to identify and respond to potential privacy incidents promptly.

A CIAM implementation can assist organizations in compliance to different controls within the privacy framework such as

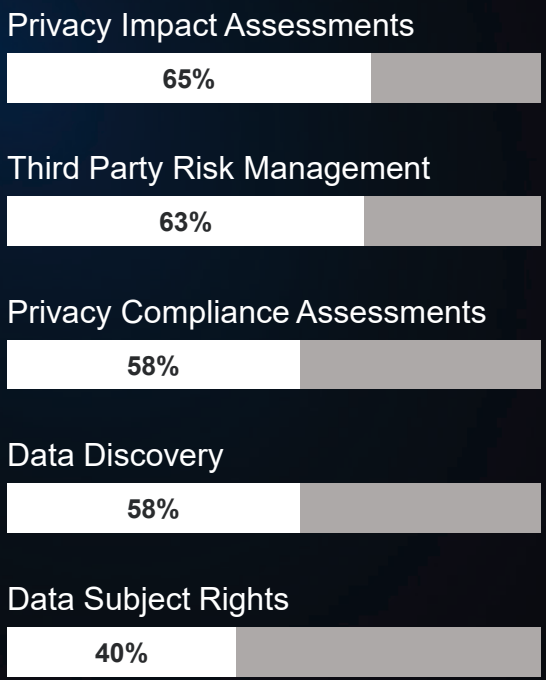
- Consent Management
- Transparency for consumers
- Enables privacy by design
- Self Service Management
- Sensitive PII data management

Road Ahead for Data Privacy in the GCC

In the next few years, we can expect organizations in the GCC to place increasing importance on data privacy, in line with global trends. This is likely to be driven by a combination of regulatory developments and growing consumer awareness on the importance of data privacy and protection.

Further, considering similar trends in cybersecurity over the last decade regular audits/ inspections can be expected from regulatory authorities to monitor an organization's privacy compliance. Organizations within the GCC also recognize these trends and around 75% of the survey respondents highlighted that improving the privacy program's GRC needs are a key investment area in 2023. The figure below indicates a few other areas where investments are being planned.

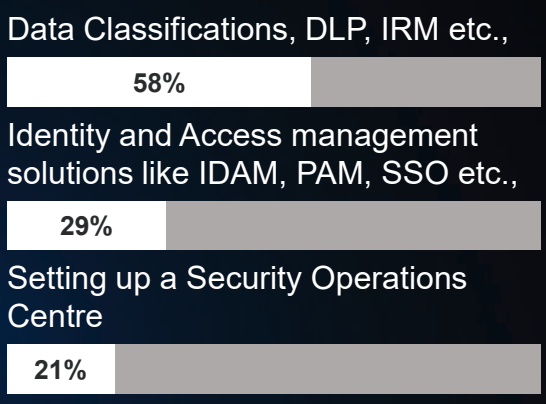
In addition to regulatory developments, we can expect to see organizations in the GCC investing in Privacy-Enhancing Technologies (PETs) to automate privacy operational activities.
As per our survey, the top 3 automation investments were Privacy Impact Assessments (rated #1), Third Party Risk Management (rated #2) and Data Discovery & Privacy Compliance sharing the 3rd spot. Figure below indicates the census on top privacy automation areas.



Data Security is another key area that is gaining significant traction. Privacy requirements are one of the key drivers pushing this agenda. The section alongside summarizes key security solutions that organizations are focusing their investments on. Interestingly, majority of the survey respondents are planning to heavily invest in Data security solutions such as Classification, DLP, and IRM.

Privacy by design is a concept that integrates privacy from the very beginning of the development of products, applications, services, and business process. For example, embedding privacy requirements (such as provisions for notice/ consent, data minimization and data retention etc.,) as part of the business requirements gathering stage.

Overall, we can expect data privacy to become an increasingly important consideration for organizations in the GCC in the coming years, as they seek to maintain compliance with new regulations and respond to changing consumer expectations.



Privacy GRC enables an organization to manage its regulatory requirements, consumer data protection needs and privacy risks. For example, establishing data privacy office and steering committee for governance and oversight,

Benefits of Privacy Program

While we have discussed multiple aspects in this whitepaper it is important to highlight the potential benefits (illustrated below) that an effective data privacy program will bring to businesses[7] as confirmed by global organizations

CONSUMER TRUST

According to a Ponemon study, 65% of individuals whose personal data was breached lost trust in the organization that experienced the breach

BRAND VALUE

A Forbes insights report stated that 46% of organizations suffered damage to their reputation and brand value as a result of a privacy breach

COMPETITIVE ADVANTAGE

Multiple organizations, in the recent past, have leveraged data privacy and protection to better market to customers and differentiate themselves from their competitors

DATA BREACH HANDLING

Adequate data security practices enable organizations to reduce security breaches. Fewer breaches translate to reduce enterprise impact

SUPPORT INNOVATION

It takes more innovation to create secure privacy- protection devices that mitigate privacy risk than it does to simply leave out such controls

7 https://www.cpomagazine.com/blogs/privacy-intelligence/12-reasons-why-data-privacy-protection-brings-business-value/

Essential Guidance

Data Privacy has transitioned from a potential consideration to becoming an important mandate and a foundational expectation by the modern consumer. Data Privacy is industry agnostic, and all businesses should embed its principles into their day-to-day business processes and service offerings. Listed below are a few key guidance aspects for businesses to consider and adopt while embarking on a data privacy program:

1. Draw out a clear strategy, operating model and roadmap to shape your program ensuring business enablement and privacy centricity.
2. Know your personal and consumer data footprint and the potential exposure to your business.
3. Understand the legal obligations (locally and globally) applicable to you with regards to data privacy and protection.
4. Adopt a risk-based approach when adopting new technologies to optimize your business operations.
5. Create leadership and employee awareness programs on data privacy, potential risks, and key potential benefits to the organization to secure their commitment and support.
6. Establish accountabilities to govern and manage your data privacy program and foster a privacy culture to create a collaborative effort towards implementing and operating your Data Privacy Program.
7. Adopt a privacy by design approach to embed privacy into key processes, business transactions and technologies.
8. Establish monitoring mechanisms to periodically check the effectiveness of the Data Privacy Program and whether it is on track to achieving the established goals and objectives.
9. Enable transparency, ease of access (to their data), and open communication to reinstate adequate control to your data subject to exercise their privacy rights.
10. Imbibe continuous improvement and promote innovation (through automation) to tackle complex challenges and optimize your program operations.

"Recognizing privacy as an intrinsic entitlement of individuals, it is incumbent upon all stakeholders to respect and uphold it. Data Privacy should not be perceived as a barrier to operations; instead, it can be an enabler for your business and be your competitive advantage"

- Niraj Mathur, Regional Leader for Security and Privacy

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Acknowledgement

Varun Kukreja, Rahul Ramesh, Oluwatosin Adunmo and Bhagyashree Ganapathi contributed to this report, led by Niraj Mathur and Siva S.

Contact Us

Abu Dhabi
Al Ghaith Holding Tower
9th Floor, Airport Road
P.O. Box: 32468, Abu Dhabi, UAE
Tel: + 9712 658 4640
Fax: + 9712 6584641
Email: abudhabi@protivitiglobal.me

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area Manama, Kingdom of Bahrain
Tel : + 973 17100050
Fax: +973 17100051
Email: bahrain@protivitiglobal.me

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
PO Box 1773, Safat 13018, Kuwait
Tel: +965 2242 6444
Fax:+965 2240 1555
Email: kuwait@protivitiglobal.me

Oman
Al-Ufuq Building, 2nd Floor
Office No.26, Shatti Al Qurum
P.O.Box 1130,P.C.112
Ruwi Muscat, Oman
Tel: + 968 24699403
Fax: +968 24696356
Email: oman@protivitiglobal.me

Egypt
Cairo Complex
Ankara Street Bureau 1
Second Floor, Sheraton Area
Heliopolis - Cairo, Egypt
Phone: +20.106.996.6659
Email: egypt@proviglobal.me

Saudi Arabia
Al-Ibdaa Tower, 18th Floor
King Fahad Branch Road, Al-Olaya, Building No. 7906, P.O. Box 3825 Riyadh, 12313,
Kingdom of Saudi Arabia
Tel: +966 11 2930021
Fax: +966 11 4615810
Email: saudiarabia@protivitiglobal.me

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE
Tel: + 9714 4380660
Fax: +9714 4380655
Email: dubai@protivitiglobal.me

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay Doha, Qatar
Phone: +974 4421 5300
Fax: +974 4421 5288
Email: qatar@protivitiglobal.me

More about us
www.protiviti.com

Face the Future with Confidence®

©2023 Protiviti Member Firm for the Middle East Region

This publication has been carefully prepared; however it should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the persons listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti Member Firm for the Middle East Region, nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this publication, or for any decision based on it.

protiviti®
Global Business Consulting