



TRUSTED VISION

Technical Proposal – PDPL Compliance

Version: 1.0

Date: 8-Feb-2026

Prepared By:

Trusted Vision for Governance and Consultation



Table of Contents

EXECUTIVE SUMMARY	3
PDPL: AN OVERVIEW	4
ABOUT US.....	5
PTM (PRIVACY THREAT MODELLING)	7
PET (PRIVACY ENHANCING TECHNOLOGY)	7
RAI (RESPONSIBLE ARTIFICIAL INTELLIGENCE)	7
PET SOLUTION AND TECH SAFEGUARDS MAPPING TO PDPL	9
PRODUCTS IN SCOPE:.....	10
1. CONSENTIUM – PROVABLE & VERIFIABLE CONSENT	10
1.1. NOTICE AND CONSENT MANAGEMENT	10
1.2. COOKIE MANAGEMENT	10
1.3. DATA PRINCIPAL RIGHTS (DPR) / DATA SUBJECT RIGHTS (DSR)	11
1.4. DATA DELETION REQUEST	11
2. PRIVACY XRAY -STRUCTURED DATA RISK PLATFORM.....	12
3. NEBULA- UNSTRUCTURED DATA DISCOVERY & RISK ASSESSMENT	12
4. PRESCRIPTION: AUTOMATED DPIA MANAGEMENT SYSTEM	13
KEY ACTIVITIES IDENTIFIED:	14
RESPONSIBILITIES & REQUIREMENTS FROM ENTERPRISE CLIENT	14
INFRA REQUIREMENT	15
SAMPLE ARCHITECTURE OF PRIVAGALAXY PLATFORM:.....	16
DETAILS OF WARRANTY	16
PAYMENT TERMS:.....	17
OUT OF SCOPE	17
CONCLUSION	18
CONFIDENTIALITY CLAUSE	18
CONTACT US.....	ERROR! BOOKMARK NOT DEFINED.



Contact Information

Please feel free to contact the following individuals for information about this document:

Name	Hashem Al-Azizi
Mobile Phone	+966-53-122-1580
Email	Hashem.azizi@trustedvision.biz
Address	Cordoba District, Saeed Bin Zaid Street, Injaz Group Building, No. 6482, First Floor, P.O. Box: 13247, Riyadh, Kingdom of Saudi Arabia



Executive Summary

THE ENTITY is currently initiating a PDPL Compliance Project for one of their key clients, and they are evaluating privacy intelligence platforms such as **Consentium, Privacy X-Ray, Nebula, and Prescriptron** from **PrivaSapien Technologies** to support PDPL alignment. These solutions collectively enable **automated data discovery and classification, cross-border data flow visualization, privacy risk prediction, structured and unstructured data protection**, helping organizations operationalize compliance with PDPL and related global frameworks.

Failure to address compliance challenges such as inadequate data subject notices, lack of breach response mechanisms, unregulated cross-border data transfers, insufficient handling of sensitive data, and absence of automated data discovery systems can lead to severe regulatory consequences. To ensure PDPL compliance, enterprises must adopt technical, organizational, and administrative measures, embedding a **Privacy by Design** approach in their operations. Article 19 of the PDPL mandates comprehensive data protection measures, ensuring that compliance is not only a legal obligation but also a driver of sustainable and secure business growth.

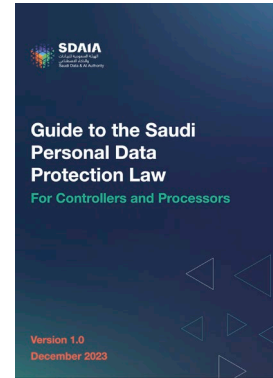
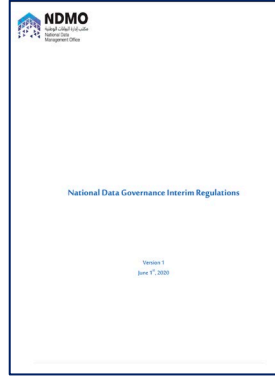
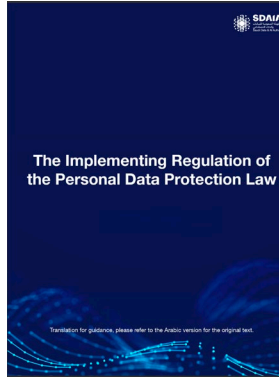
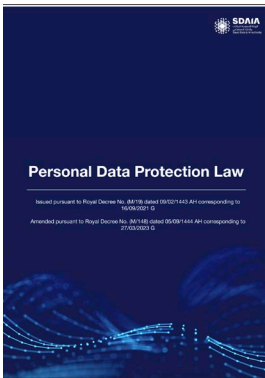
PrivaSapien, recognized by **SDAIA through the Regulatory Privacy Sandbox**, is well-positioned to support enterprises like THE ENTITY in achieving PDPL compliance through its advanced privacy-enhancing technologies. By leveraging PrivaSapien's products THE ENTITY can establish a robust privacy governance framework that ensures compliance, safeguards data assets, and enhances stakeholder trust across its operations.

Please note that this document is a **sample technical proposal** and **not the final version**. A fully reviewed and finalized proposal will be provided after our detailed discussion with the client.

PDPL: An Overview

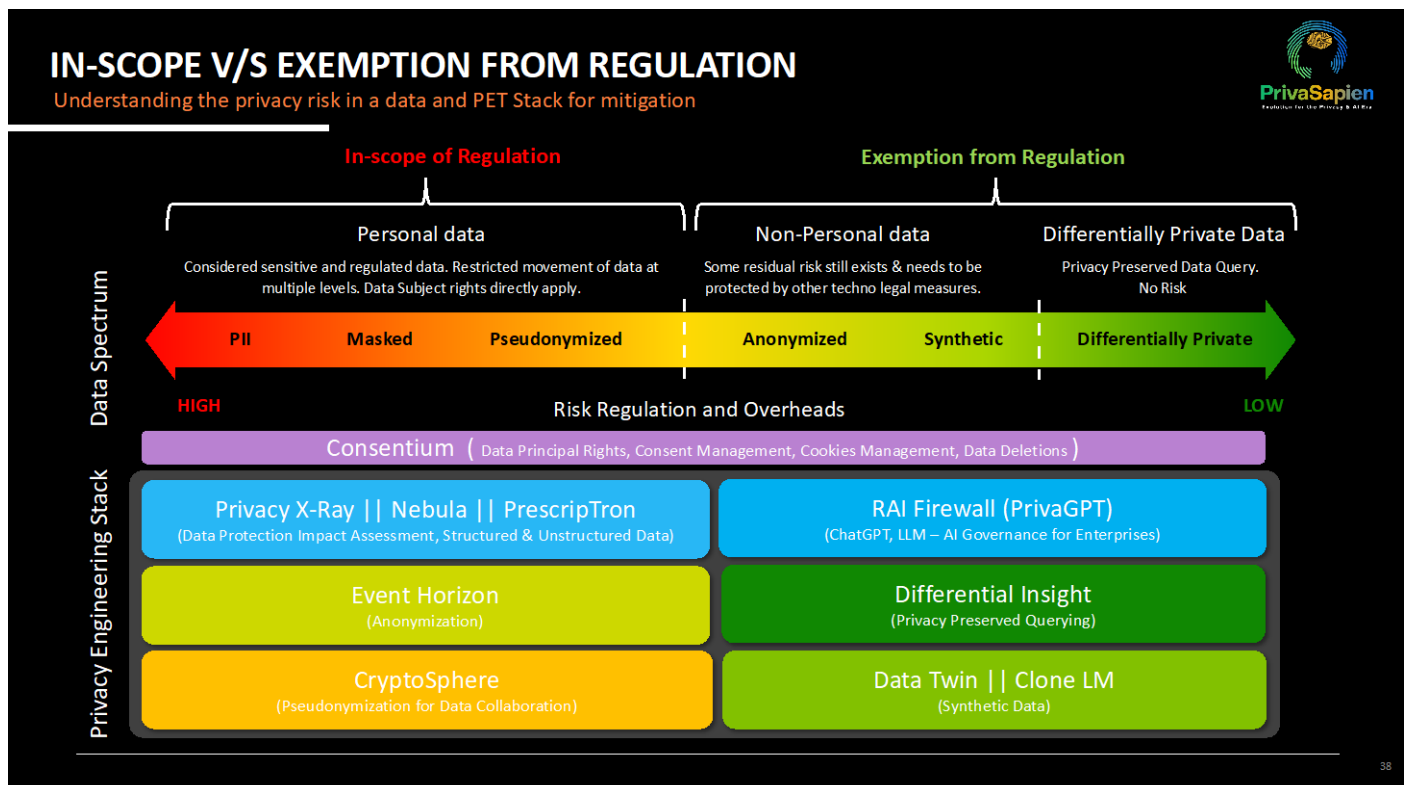
Aligned with the Kingdom of Saudi Arabia's Vision 2030, which aims to transform and develop digital infrastructure in the public and private sectors, law to regulate "Personal Data" of people residing in the Kingdom came into force on 14 Sep 2023, known as PDPL with its set of implementing regulations (formally issued on 07 Sep 2023). PDPL initially implemented on **16 September 2021** (vide Royal No. M/19 of 9/2/1443 AH) and amended **on 27 Mar 2023** (vide Royal Decree No. M/148 of 05/09/1444 AH), called as the **implementing decree**, gave entities covered under the ambit of PDPL a **grace period/ time window of one year to adjust their status of compliance with the PDPL effective from 14 Sep 2023**. It is expected that the **controllers shall correct their data protection posture by 14 Sep 2024**.





About Us

Trusted Vision is a partner with PrivaSapien, which is a pioneering Privacy engineering company with award winning Privacy enhancing and responsible AI technology products. PrivaSapien empowers businesses in building digital trust with their customers by implementing “Privacy by Design” in their data ecosystem. They ensure businesses are able to unlock data while being compliant to global privacy regulations like PDPL, GDPR, CPRA, PDPL etc and enhance digital trust. Digital trust is the new foundation of long-term customer relationship and for creating new age digital and AI services for customers.





They Provide a powerful platform of privacy-enhancing tools that can help businesses evaluate privacy risk, mitigate privacy risk and unlock the data for value creation across the enterprise data ecosystem. The platform hosts solutions across 3 categories: Privacy Threat Modelling, Privacy Enhancing Technologies and Responsible AI Technologies which include products like Privacy X-Ray, Prescriptron, Nebula, Event Horizon, Data Twin, Crypto Sphere, Differential Insight, RAGAM and RAIFireLMs.





PTM (Privacy Threat Modelling)

It is a systematic approach used to identify, assess, and mitigate privacy risks within an organization's data processing activities.

Features

- Consent Management, Data Subject Rights, Data Deletion Requests
- Identifying and classifying Data Assets
- Identifying Privacy Threats & Vulnerabilities
- Assessing , quantifying and visualizing Risks
- Recommendation mitigating controls as per Regulations
- Conduct augmented DPIA
- Reporting and Dashboard

Products: Consentium, Privacy Xray, Nebula and Prescriptron

PET (Privacy Enhancing Technology)

PETs are technologies designed to protect individuals' privacy by minimizing the collection, use, and disclosure of personal data, while still allowing for the functionality and utility of systems and services.

Features

- Data Minimization
- Data Anonymization
- Synthetic Data Generation
- Data Pseudonymization
- Differential Privacy
- Mathematical Proofs

Products: Event Horizon, CryptoSphere, Data-Twin/ CloneLM, Differential Insight

RAI (Responsible Artificial Intelligence)

RAI refers to the ethical and accountable development, deployment, and use of AI systems. It encompasses a set of principles by NIST that prioritizes fairness, transparency, accountability, safety, and societal well-being.

Features

- Safe AI
- Secure AI
- LLM Governance
- RAG – Data Annotation
- Tokenization
- Redact
- Encryption

Products: RAIFireLMs & RAGAM





Privacy Management



Consentium
Provable & Verifiable Consent
& Data Lifecycle Mgmt

PTM



Privacy X-Ray
Automated Privacy Threat
Modelling & Risk Assessment



Nebula
Unstructured data risk
discovery



Prescriptron
Augmented DPIA

PET



CryptoSphere
Pseudonymization &
Cryptographic Collab



EventHorizon
Contextual Anonymization
with Proofs



DataTwin
Synthetic Data for
Application Testing



CloneLM
Synthetic Data for model
building



Differential Insight
Differentially Private insight
sharing

Responsible AI



PrivaGPT
Gen AI & LLM Governance for
enterprise

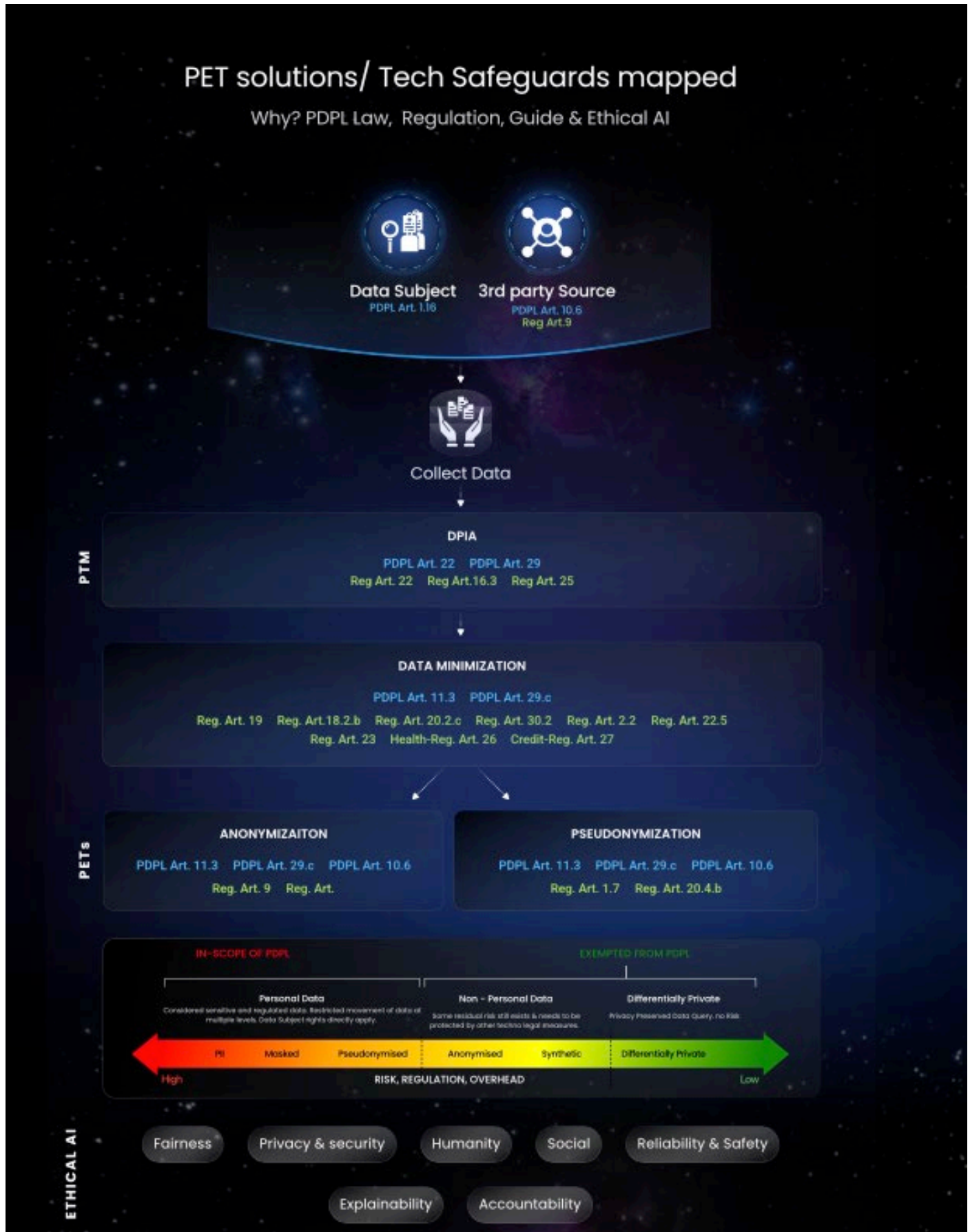


Ragam
Unstructured data risk
mitigation for LLMs & RAG





PET Solution and Tech Safeguards Mapping to PDPL





Products in Scope:

Based on comprehensive analysis of the Saudi Data and Artificial Intelligence Authority (SDAIA) guidelines for PDPL implementation, **PrivaSapien** identifies the following integrated solutions to be deployed within **enterprise environments** for comprehensive PDPL compliance:

1. Consentium – Provable & Verifiable Consent :

1.1. Notice and Consent Management :

Consentium's Consent Manager module is designed to ensure compliance with global privacy regulations, offering a comprehensive, user-friendly platform for managing consent.

- **Regulatory Compliance:** Ensures adherence to regulations like PDPL, DPDPA 2023, GDPR, etc, covering the complete spectrum of consent requirements.
- **Centralized Dashboard:** Provides a holistic view of all consents, applications, and purposes in a single interface.
- **Granular Control:** Allows users to add, or withdraw consent for different purposes, ensuring alignment with privacy principles like purpose limitation and data minimization.
- **ROPA Management:** Maintains Records of Processing Activities (ROPA) and maps consents to specific applications, purposes, and responsible teams.
- **Formal Approval Process:** Supports a digital signature and timestamp process for consent approvals and consent verifiability.
- **Real-Time Tracking:** Monitors the current status of consents (Withdrawn/Not Withdrawn) with real-time updates.
- **Comprehensive Integration:** Seamlessly integrates with applications, Data Protection Impact Assessments (DPIAs), teams, and associated forms, offering end-to-end consent management.
- **Consent Withdrawal Workflow:** Streamlines the process for users to revoke consent, ensuring a quick, transparent, and efficient withdrawal experience.

1.2. Cookie Management:

Consentium's Cookies Management module provides dynamic, customizable control over cookie consents, ensuring that users and organizations remain compliant with privacy regulations.

- **Fully Customizable Interface:** Allows businesses to tailor the layout, colours, and style of the consent management portal to match their branding.



- **Regulatory Compliance:** Complies with PDPL, DPDPA, GDPR, etc to manage cookie consent effectively.
- **Categorized Cookie Management:** Enables users to accept or reject cookies by category (e.g., Strictly Necessary Cookies, Functional, Marketing/ Targeting, Performance Cookies etc).
- **Granular Cookie Control:** Offers users the ability to manage individual cookie preferences with detailed information on each cookie, including name, provider, purpose, and expiration.

1.3. Data Principal Rights (DPR) / Data Subject Rights (DSR) :

Consentium's DPR solution offers a centralized platform to manage all data subject rights, ensuring compliance with privacy regulations.

- **Right to Erasure (Forgetfulness):** Provides a streamlined process for users to request the deletion of their personal data across various applications.
- **Right to Restricted Processing:** Allows granular control over limiting data processing for specific purposes or applications.
- **Right to Access:** Enables users to view comprehensive details of their consents, including purposes, applications, and timestamps.
- **Centralized Management:** A unified dashboard that supports efficient management of various DSR requests, integrated across websites, apps, and customer-facing platforms.

1.4. Data Deletion Request :

Consentium's Data Deletion Request process streamlines user requests for consent withdrawal and data erasure, ensuring regulatory compliance and transparency.

- **Unique Reference Number:** Each request is tracked with a unique reference number for better auditability.
- **Evidence Collection:** Supports evidence gathering for data deletion requests.
- **Visual Tracker:** Offers a visual status tracker for all withdrawal requests, allowing users to monitor progress in real time.
- **Audit & Reporting Panel:** Provides detailed insights into the status of deletion requests for compliance and reporting purposes.





2. Privacy Xray -Structured Data Risk Platform:

To understand privacy risks associated with both direct and indirect identifiers, **Privacy Xray** has developed a novel method of privacy threat modelling and privacy attack simulation to provide mathematical risk scores, automated technical and regulatory recommendations, enabling accelerated governance, augmented DPIA, and a verifiable process for unlocking structured data.

Scope: Analysis and discovery across approximately **300- 400 structured tables**.-mssql

Key Capabilities:

- **Automated Data Discovery:**

- AI-driven scan across structured databases, applications, and endpoints to identify PII/PHI.
- Predefined and custom risk tags with automated ranking and policy engine triggers.
- Role-based dashboards with logs and forensics for audit-ready artifacts.

- **Data Classification & Risk Mapping:**

A fully automated process enabling the Data Protection Officer (DPO) to identify and classify data, assess risks, and retrieve reports on sensitive and personal data across connected databases.

- **Risk Mapping:**

Identify and visualize data risks to ensure proactive compliance management.

- Categorizes personal, sensitive, health, and financial data by regulatory context (PDPL).

3. Nebula- Unstructured Data Discovery & Risk Assessment:

Nebula identifies direct identifiers in unstructured data and categorizes the context of sensitive information such as financial, health, or other confidential organizational information. It quantifies the risk, thereby empowering organizations to accelerate governance, recommend mitigation, and enable secure data flows in complex unstructured data environments.

Scope: Sensitive data discovery in files for approximately **100 GB**.

Key Capabilities:

- **Unstructured Data Risk Identification:**

Assess and identify risks associated with unstructured data, ensuring compliance across non-database data sources.

- Over 95% detection accuracy in identifying relevant data points, PII, PHI, and personal sensitive information.





- Supports category-wise tagging (PII, PHI, etc.) with high-risk file clustering capabilities.
- **PII Annotation and Classification:**
PII annotation and classification across various file types such as DOCX, PDF, TXT, and log files.
- **Discovery and Auditability:**
Discovery logs and scan versioning with tenant-based scanning for multi-entity environments.
 - Automatic PII detection and classification to ensure secure handling.
 - Automated generation of compliance reports and documentation for audits.

4. Prescriptron: Automated DPIA Management System:

PrescripTron is a powerful tool for DPOs where the approval process is tightly integrated with privacy threat modelling results, business requirements, and automated technical and regulatory recommendations. It augments DPOs in approving DPIAs in a quantifiable, verifiable, and auditable way.

Scope: Management of approximately **200 DPIAs**.

Key Capabilities:

- **Automated Risk Assessment:**
Embedded lifecycle with a scoring engine aligned with PDPL Articles 29–31 DPIA obligations.
 - Risk heatmaps and DPIA benchmarks with impact tiering for decision-making.
 - DPIA templates and thresholds with custom organizational configurations.
 - Decision trail maintenance with structured justification per Nature, Purpose, Scope, and Context.
- **Regulatory Documentation:**
 - Versioning and audit trail with complete history of risk changes and stakeholder approvals.
- **Consentium:**
 - **Consent Management:** Automated consent management, integrating with various online and offline platforms to collect, record, and display consents efficiently.
 - **Data Subject Requests (DSR):** A fully automated DSR workflow where the tool links with the front end to collect requests and displays them as Requests/ tickets within the tool.





Key Activities Identified:

- Usage of the PrivaSapien solutions (Consentium, Privacy X-ray, Nebula and Prescriptron) to support PDPL compliance.
- Granted Limited License for all products for a single deployment.
- PrivaSapien will train THE ENTITY teams on using the solutions for one application completely.
- Basic Support is provided for the deployment.
- Following the training, the THE ENTITY team can start using the solutions and can reach out to the PrivaSapien team for any queries or support.
- Privacy X-ray works on sampling.
- Nebula for Unstructured Data Risk Identification and supports unstructured data formats, including PDF, DOC, and TXT files.
- Layout and UI preservation in the supported formats (e.g., PDF, DOC) is not guaranteed and is subject to customer discretion. We can work as per the customization requirements and work with THE ENTITY teams on this.
- The solutions support structured data formats – CSV, JSON, and XML, within the project scope.
- The solutions are compatible with databases/data lakes using the above structured data formats in MySQL, Oracle DB, Azure, PostgreSQL, MongoDB, DocumentDB, and S3 bucket. Any additional integration might be considered as customizations and will be charged as per complexity and efforts.
- **Currently only English language is supported Out of the Box** and considered in scope. Any Additional language support would require co-creation activities with the client which is chargeable as per efforts and complexity and can be discussed separately based on the requirements.
- Product customization, including layout changes in **DPIA templates**, will be subject to the limitations of the product and may result in adjustments. These customizations will be charged separately based on the complexity of the requirements.

Responsibilities & Requirements from Enterprise Client:

- **Infrastructure:** THE ENTITY is responsible for provisioning the Kubernetes cluster and other required infrastructure as outlined in the shared documentation.
- **SSL Configuration:** THE ENTITY will provide the SSL certificates necessary for secure configuration.
- **DNS Mapping:** Collaboration between THE ENTITY and **PrivaSapien** will be required for the DNS mapping setup.
- **Azure Active Directory:** THE ENTITY will assist with configuring AD for user access management.
- **API Integration:** Support from THE ENTITY will be required to understand the system integration needs, particularly for API-related modules.



- **Workflow Logic and Approvals:** THE ENTITY will facilitate discussions around workflow logic and approval mechanisms for DPIA and risk modules.

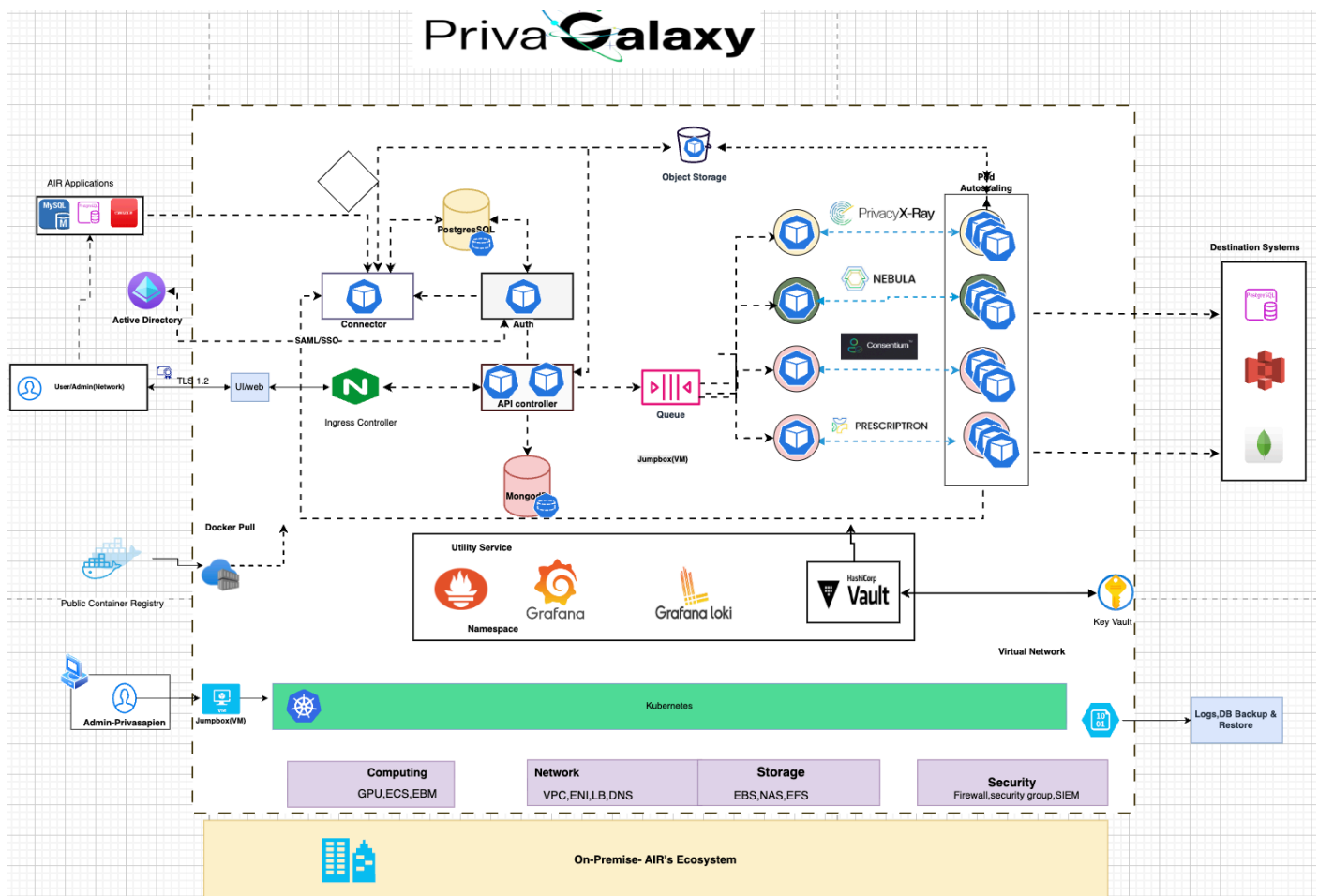
Infra Requirement:

Below is the high-level sample Infra requirements for solutions based on standard consumption. This is subject to change based on the discussion with Enterprise Client (Considering On prem server). We will deploy the solution on your GKP server, for which access to the GKP cluster will be required.

On Prem Kubernetes Resource Requirement						
Node Type	No of Instance	CPU	GPU	RAM	Storage	OS
Master	3	8	NA	32	500GB	Ubuntu : 24 LTS
Worker	4	16	NA	64	500GB	Ubuntu : 24 LTS
GPU-worker	3	4	24GB	16	500GB	Ubuntu : 24 LTS
Storage						
Type	Size					
NFS	100GB					
Jump Server						
Instance Type	No of Instance	CPU	GPU	RAM	Storage	OS
For Clusture Access	1	4	NA	16	500GB	Ubuntu : 24 LTS
Other Requirements						
Container Registry - To store container images						
SSL Certificate - For Secure Connection						
DNS						



Sample Architecture of Privagalaxy Platform:



Details of Warranty

- **Scope:** The warranty covers any defects in software or workmanship under normal use during the warranty period.
- **Duration:** The warranty period of tokens starts from the date of delivery and lasts for **12 months**, unless otherwise specified at the onset of the project.
- **Included Services:** The warranty includes support for bug fixes, software patches, and updates to ensure the software remains functional, secure, and compliant with regulatory standards.
- **Indirect Damages:** **PrivaSapien** is not liable for any indirect, incidental, or consequential damages arising from the use or inability to use the software.
- **Maximum Liability:** The maximum liability of **PrivaSapien** under this warranty is limited to the amount paid by **THE ENTITY** for the software.
- **Maintenance and Support:** As per the Service Level Agreement (SLA).



- **Contact Information:** For the timely delivery of this project, necessary access requirements must be in place in the deployment ecosystem.
- **Support Team:** **THE ENTITY** can reach the support team via email or phone, only for critical incidents and emergencies, available as per the support plan opted for.
- **Escalation:** For unresolved issues, **THE ENTITY** can escalate to **PrivaSapien** as per the agreed escalation path.

Payment Terms:

- An advance payment of the full licensing fee annually is required upon signing the agreement to initiate access to the licensed products and services.
- This pricing offer is a special, one-time arrangement applicable for the timeline provided for the engagement. It may expire and PrivaSapien reserves the rights to change it based on its discretion if not aligned previously.
- The current scope of the project and pricing are defined for the time provided only, which includes a significant discount. If Partner or Customer wishes to extend the contract, we can initiate a formal discussion review the terms and agree on pricing for the subsequent period.

Out of Scope

- **Infrastructure Cost:** Infrastructure costs are considered out of scope in this proposal. This includes expenses related to the procurement, setup, maintenance, and operational costs of hardware, software licenses, cloud services, and any associated infrastructure needed for project implementation.
- **Changes to Scope Post-Gap Assessment:** Any changes or additions to the project scope following the gap assessment will require a formal review and approval process. This ensures alignment with project objectives, resource availability, and stakeholder expectations, maintaining transparency and accountability throughout the project lifecycle.
- **Out-of-Scope Features:** Certain feature requirements fall outside the scope of the service provider and are indicated in red. These functionalities are not part of the contractual obligations and will not be delivered as part of this engagement.
- **THE ENTITY Responsibility for Infrastructure & Team Availability:** THE ENTITY is responsible for infrastructure provisioning and ensuring the availability of their team for workshops and training sessions. Our services will include conducting workshops and training, but we expect the relevant teams to be present and actively engaged.





Conclusion

In conclusion, our proposed solution is tailored to meet Enterprise Client's unique needs and drive success. We are committed to delivering excellence, collaborating closely to turn challenges into triumphs. Thank you for considering our proposal we look forward to the opportunity to architect a privacy by design ecosystem contribute to Enterprise Client's success.

For more information, please feel free to write to contact@privasapien.com

Confidentiality Clause

We recognize the sensitivity of the information shared during this engagement, including budgetary details and the nature of the product outputs and deliverables. Therefore, both parties commit to maintaining the strictest confidentiality with regard to any financial details, estimates, or discussions. This information will not be disclosed to any third parties without explicit written consent from both parties, except as required by law.

